91602
new 82-10

LEGAL NOTICE

This report was prepared by Ontario Hydro and, while effort has been made to assure the accuracy and applicability of the material contained herein, neither Ontario Hydro nor any person acting on its behalf:

(a) makes any warranty, express or implied with respect to the use of any information, apparatus, method or process disclosed in this report or that such use may not infringe privately owned rights; or

(b) assumes any liabilities with respect to the use of, or for damages resulting from the use of, any information, apparatus, method or process disclosed in this report.

89-04811/

ontario hydro
research division

COMMENTARY COPY

CLARKSON SCC RELIABILITY ASSESSMENTS

Report No. 89-69-K

L. Wang
Senior Engineer - Reliability
Reliability & Statistics Section
Operations Research Department

ABSTRACT

The control and data processing facilities in the new System Control Center (SCC) at Clarkson consist of the data-acquisition and control-action subsystem (DAS/CAS), the computer subsystem (CS), and the man-machine subsystem(MMS). The new SCC building is serviced by a specially designed heating, ventilating and air-conditioning (HVAC) system. The power needs of the new SCC are provided by a power supply subsystem (PS) which consists of supplies from the bulk electricity network, with emergency power from combustion turbine units. The reliabilities of these subsystems and the probabilities of successfully carrying out specified SCC functions using these subsystems were assessed. The results of these assessments, as described in this report, show that the reliability targets wherever given are generally met.

job	file	date	report no.
72-202-422	813.07	February 28, 1989	89-69-K

TABLE OF CONTENTS

1. Introduction

2. System Composition

3. Reliability Assessment Approach

4. Subsystem Reliability
   4.1 The Heating, Ventilating and Air-Conditioning Subsystem
   4.2 The Power Supply Subsystem
   4.3 The Computer Subsystem
   4.4 The Data Acquisition and Control Action Subsystems
   4.5 The Man-Machine Subsystem

5. SCC function Reliability

6. Conclusion

Appendix A. Computer Subsystem Reliability computations

Appendix B. DAS/CAS Subsystem Reliability computations

Appendix C. Man-Machine Subsystem Reliability computations

Appendix D. SCC Function reliability computations

Attachment 1. "Reliability Assessment of the HVAC System for the Clarkson System Control Center" by L. Wang, Research Division Report No. 88-219-K, September, 1988.

Attachment 2. "Reliability Assessment of the Power Supply for the Clarkson System Control Center" by N. Ramani, Research Division Report No. 88-304-K, December, 1988.

ontario hydro
research division

To: Mr. R. C. Seaton
Project Manager
System Control Center Relocation Project Department
Design and Development - Transmission

CLARKSON SCC RELIABILITY ASSESSMENT

1. INTRODUCTION

The new System Control Center (SCC), now under construction at Clarkson, is scheduled for service in 1991. The control facilities in the new SCC are designed to make use of the state-of-the-art technology in data processing, electronics, control, and service equipment. Although the intended functions of the new SCC are similar to the existing ones, the equipment to be used in performing these functions will be quite different. It is essential that the new design should meet the specified levels of reliability.

At the request of the System Control Center Relocation Project Department, reliability assessments were carried out for the various systems and functions of the new SCC. The models and methods used in the assessment and a summary of the results are presented in this report.

2. SYSTEM COMPOSITION

The facilities at the new SCC consist of the following: The data acquisition subsystem and control action subsystem (DAS/CAS), the computer subsystem (CS), the man-machine subsystem (MMS) and the power supply subsystem (PS). These subsystems constitute the data acquisition and computer system (DACS), which will be housed in a new three-story building under construction at Clarkson. This building will be serviced by a heating, ventilating and air-conditioning (HVAC) system, which provides the necessary operating environment for the DACS equipment and the operating personnel.

3. RELIABILITY ASSESSMENT APPROACH

The DACS facilities at the new SCC will be used in performing a variety of operational and support functions. Some of these functions are essential to the successful operation of the power system; others are less important. Hence reliability requirements for these different applications also vary. After discussions with the clients, it was decided that reliability assessments will be carried out for all the subsystems first. The combined reliability of the subsystems needed for successfully carrying out a specific function will then be assessed using the information obtained for the subsystems. A list of the functions to be studied has been given by the user in PSOD.

Each of the subsystems of DACS at the new SCC is very complex. The levels of redundancy vary from subsystem to subsystem, and also from point to point within a given subsystem. Almost all of the subsystems have multiple "input" and "output" points. These characteristics make it difficult to apply a systematic approach to the reliability assessment of the subsystems. The state enumeration method is used in this study. Approximations were made by limiting the level of contingencies included in the computations when it was evident that higher contingencies would not contribute significantly to the computed reliability indices.

Assessments were carried out for the specified pairs of input and output points of the DACS subsystems. The reliability of a given SCC function can be computed by considering the subsystems needed in performing this function to be connected in series.

4. SUBSYSTEM RELIABILITY

The results of the reliability assessments for the subsystems are summarized in this Section. Details of the assessments are given in Appendixes A to D and Attachments 1 and 2.

4.1 The Heating, Ventilating and Air-Conditioning Subsystem

A simplified diagram of the HVAC system is given in Figure 1. Cooling is provided by 3 water chillers, any two of which can carry the air-conditioning load of the SCC. Any one chiller can be operated to provide adequate cooling capacity for the essential loads, ie the control room, the computer room and the electrical equipment room. Chilled water is circulated to the air handling units where air is cooled and circulated to the required load areas. Redundant air handling units and additional back-up capabilities are provided for the essential load areas.

It is expected that the air-conditioning system for the essential load areas will operate in the cooling mode all the year round. During the winter season, much of the energy required for space heating in the administration area can be obtained from recovering the heat rejected by the operating water chillers. Supplementary heating is provided by fan coils and an electric boiler.

The predicted unavailabilities, the mean times between failures (MTBF) and the mean down times of the air conditioning systems for the four load areas of the new SCC are given in Table 1, with the reliability targets given in brackets following the computed indices.

TABLE 1

HVAC System Reliability Indices

Load area	Unavailability	MTBF, yr.	Mean down time, hr.
Control room	5.09E-6 (9.0E-5)	64 (5)	2.86 (4)
Computer room	5.09E-6 (5.7E-6)	64 (10)	2.86 (0.5)
Electrical equip rm	5.09E-6 (5.7E-6)	64 (10)	2.86 (0.5)
Admin area	0.83E-3 (-)	1.2 (-)	4.77 (-)

The results in Table 1 show that the unavailability and the MTBF indices for the essential load

areas (the control room, the computer room, and the electrical equipment room) are well within the specified reliability requirements. The mean down times of air-conditioning systems for the computer room and the electrical equipment room are longer than the specified values. An air-conditioning system failure in an essential load area can occur only when several components in the HVAC system fail simultaneously, exhausting all redundancies in the system. In such a case air-conditioning service can be restored only by completing the repair work of at least one of the failed components. It is unlikely that the mean repair times of the HVAC system components can be reduced significantly. Hence the specified mean down time of 0.5 hour for the computer room and the electrical equipment room air-conditioning systems may prove to be difficult to meet.

An interruption of power supply to the HVAC system would cause it to stop functioning. The probability of occurrence of this event is approximately 2.0E-9, with a mean downtime of 4.0 hours.

As mentioned before, the HVAC system for the new SCC is designed with a high degree of redundancy. An air-conditioning system composed of components identical to those in the HVAC system for the new SCC but with no redundancy has an unavailability of 2.91E-3 (equivalent to a failure frequency of 4.72 times per year and a mean down time of 5.41 hours). This simple example shows that the high reliability levels of the HVAC system for the new SCC are achieved through redundancy. Real-life experience confirms that most air-conditioning systems with no redundancies perform much more reliably than the one given in the above example. This suggests that the results obtained in this assessment are not overly optimistic.

A detailed description of the HVAC system reliability analysis is given in Attachment 1.

4.2 The Power Supply Subsystem

The new SCC is supplied by feeder M13 from Oakville TS and feeder M4 from Lorne Park TS, as shown in Figure 2. These two sources can be considered independent when no serious disturbances are present in the bulk power system.

The two 27.6 kV feeders are the starting points of two parallel supply paths. Each supply path consists of a 27.6/4.16 kV step down transformer, a 4.16 kV bus, a Class III unit substation and a Class IV unit substation, and ties between the two paths are provided at these three points. Two combustion turbine units (CTUs) are provided for emergency power when the supply from the transmission system is interrupted. The CTUs are connected to the Class III buses, as shown in Figure 3. The DACS facilities in the control room and the computer room are supplied from two uninterruptible power supply (UPS) units A and B, backed up by UPS C. UPS units D and E supply power for the switchgear and other critical loads. The UPS system includes storage batteries which supplies emergency power before the CTUs are brought on line.

A number of load points are defined to facilitate the reliability assessment process. These loads points are described below:

Load points:

T1	Load supplied by a feed from a Class IV substation.
T2	Load supplied by a feed from a Class III substation.
T3	Load supplied by feeds from both Class III substations.

T4	The output of the UPS A switchgear.
T5	The input to a computer distribution frame feeding the computer and control rooms.
T6	Any one of the four feeds to the computer room.
T7	Two of the four feeds to the computer room, the two feeds in question being fed via two separate computer distribution frames.
T8	Any one of the two feeds to the control room.
T9	Both the feeds to the control room.
T10	Any one of the three feeds to the DACS support system.
T11	The output of UPS D (or UPS E) computer distribution frame.

The reliability indices of power supply to the load points listed above are summarized in Table 2. In this Table, the results include supply interruptions caused by forced outages alone and those caused by forced outages of a backup during a maintenance. Momentary outages are not included. It should be noted that if the maintenance of a component causes an immediate outage at any of the load points, then this event is not included in the results for that load point, but is included in all downstream calculations. For example, the maintenance of UPS A switchgear causes an immediate outage at load point T4, and the result for T4 in Table 2 does not include the impact of this event. However, this maintenance event does affect load point T6, and the impact of this event is included in the results for T6.

A more detailed description of the power supply subsystem reliability analysis can be found in Attachment 2.

Note that criteria for supply reliability at these load points have not been specified. The results of the reliability assessment have been deemed acceptable by the designers and users based on their experience and judgement.

TABLE 2

Reliability of Power Supply to SCC Load Points

Load Point	MTBF (years)	Mean Time to Restore	Probability of Outage
T1	2.13	1.46 hrs	$78.5 * 10^{-6}$
T2	208	8.00 hrs	$4.39 * 10^{-6}$
T3	200,000	4.00 hrs	$2.02 * 10^{-9}$
T4	75.4	7.62 hrs	$11.5 * 10^{-6}$
T5	75.3	10.6 min	$0.267 * 10^{-6}$
T6	18.3	12.8 hrs	$79.8 * 10^{-6}$
T7	500,000	3.76 hrs	$0.854 * 10^{-9}$
T8	23.9	8.65 hrs	$41.3 * 10^{-6}$
T9	1,000,000	3.66 hrs	$0.429 * 10^{-9}$
T10	26.0	17.0 hrs	$74.8 * 10^{-6}$
T11	118	4.64 hrs	$4.49 * 10^{-6}$

4.3 The Computer Subsystem

The cumputer subsystem consists of two groups, one for on-line operations and the another for support and development functions. The on-line group has six computer nodes; any three of the six nodes can be designated for LIVE operations and the remaining three nodes serve in the QA role. The main computer for each of the on-line nodes is a two-processor Liberty system from UNISYS. All the on-line nodes are linked via a high speed LAN (Hyperchannel), comprised of four trunks and an adapter for each node. Two of the trunks are dedicated to LIVE operations, the remaining two trunks are used by the QA function. The LIVE nodes have access to two disk strings, which contain identical files necessary for all the on-line operation functions. Two other disk strings are provided for the backup function. The LIVE nodes can have access to the backup strings in case of failure of a live string. The nodes are designed to be self-contained so that possible interactions between them are minimized. A block diagram for the on-line computer configuration is shown in Figure 4.

The functions of the three LIVE nodes are, respectively, real-time monitoring and control (R/T), security and economic assessment, and study and forecast. The QA cluster is designed to run in parallel with the LIVE cluster and "listens" to the data from the RTUs. In the event of a R/T or assessment node failure, the functions will be taken over automatically by the Study node or by the manual switching of another node in the QA cluster which is already operating.

The computer system for support and development functions also consists of three nodes. One of the three has four processors; the remaining two are of the two-processor type. The Hyperchannel will be configured with two trunks only. The disk configuration has less redundancy than the on-line system, so are the other peripherals. A block diagram of the computer subsystem for support and development is shown in Figure 5.

Reliability assessments were made for all three computer nodes of the on-line group and those of the support function group. The outage of a computer node can be caused by hardware failure, software failure or planned outage. In assessing the on-line computer nodes, considerations were given to the automatic switch-over of the R/T or Assessment node to the Study node and the waiting times of the lower priority nodes whenever the R/T node is interrupted. Because of the availability of the QA nodes in the on-line group, the effect of repairing hardware failures is considered negligible in the reliability computations. No automatic switch-over is possible in the support function group. The R/T node in this group can operate in a degraded state if one of its four processors becomes unavailable. Repairs are needed to restore operation in most cases of hardware failures for the other two nodes.

The computed reliability indices for the computer nodes are summarized in Tables 3A and 3B. Details of the reliability computations are given in Appendix A.

An 1.5-hour outage of the R/T node of the on-line system will occur when a LIVE disk unit and its backup in the second disk string develop overlapping failures. The Probability of occurrence of such an event is quite small (3.28E-7), with a mean time between failure of 522 years.

4.4 The DAS/CAS Subsystem

The DAS/CAS subsystems consist of four data communication processor (DCP) blocks, as shown in Figure 6. Any two of the four DCPs can be used for LIVE operation, the remaining two DCPs serve as quality assurance (QA). Each DCP is made up of a communication processor, a modular memory unit, and a number of input-output modules. Each input-output module can hold up to

TABLE 3A

On-Line Computer Subsystem Reliability Indices

	Outage Category									
	0-1 Minute		1-5 Minute		5-15 Minute		Planned		Overall Outage	
Node	Freq*	Unavail	Freq	Unavail	Freq	Unavail	Freq	Unavail	Freq	Avail
R/T	23.9	0.000045	0.000055	3.15E-10	0.0	0.0	24	0.000045	47.9	0.99991
Assessment	23.7	0.000044	23.9	0.000136	0.0	0.0	88	0.000258	135.5	0.9996
Study	18.0	0.000034	29.3	0.000278	23.9	0.000363	88	0.000258	159.2	0.9991
QA	-	-	-	-	-	-	-	-	32.85	0.9755

TABLE 3B

Support Function Computer Subsystem Reliability Indices

	Outage Category							
	5-Minute		Full Forced		Planned		Overall Outage	
Node	Freq	Unavail	Freq	Unavail	Freq	Unavail	Freq	Avail
R/T	18	0.000171	3.56	0.00229	24	0.000228	45.6	0.9973
Assessment	18	0.000171	5.72	0.00429	88	0.0296	111.7	0.9659
Study	18	0.000171	5.72	0.00429	88	0.0296	111.7	0.9659

* All frequency indices are in occurrences per year.

16 line modules. The DAS portion of each of the DCPs has two paths, A and B, each of which consists of 50 RTU (remote terminal unit) loops initially. The number of RTU loops can be expanded to 100 in the future. The CAS portion of the DCP provides 30 AGC (automatic generation control) output ports initially, and is expandable to 96 ports. The layout of the QA section is identical to that of the LIVE section.

The basic assumptions for the DAS/CAS subsystem reliability assessment are:

(1) If there is only one component failure in the system and it occurred outside normal working hours, repair work will not commence until the next normal working day. Repairs will start as soon as poosible when a second component has failed. In actual operation, repair delays of some double contingency failures may be tolerated if the operators believe that the integrity of DACS operatios is not threatened.

(2) Manual switchover to the QA section will be made when the LIVE section stops functioning.

The results for the DAS/CAS subsystem is given in Table 4. The details of the reliability computations are given in Appendix B.

TABLE 4

DAS/CAS Subsystem Reliabillty Indices

Function	Failure Freq., per yr.	Availability
LIVE	0.097	0.999997
QA	0.107	0.999997

Note that the above results for DAS/CAS do not include failures in the communications network. Experience in the past shows that the effect of failures in the communications network on DACS operations is negligible.

4.5 The Man-Machine Subsystem

The man-machine subsystem consists mainly of devices for inputting control commands (keyboards) and devices for displaying the status of the power system (CRTs, wall diagram). It consists of three parts, as shown in a block diagram in Figure 7. The first part of the MMS is located in the control room, to be used by the control supervisors and the system control engineer. The facilities include 24 CRTs, 9 display generators, 6 keyboards, and a wall diagram. Power system data processed by the computer subsystem is fed to the control room via two interface units. Information to be displayed on the wall diagram is processed by one of two fully redundant routes.

The second part of the MMS is to be used by the off-shift support staff of the System Operation Department. It has 7 Display generators (providing 28 video channels), 24 CRTs, 2 projection CRTs for the public viewing gallery, and 9 keyboards. Some of these facilities will also serve as a backup for the control room.

The third part of the MMS is for software maintenance and development. It consists of 8 display generators, 24 CRTs and 14 keyboards. Interfaces with both the ON-line and the support sections of the computer subsystem are provided.

The built-in redundancy in the subsystem is such that, in most cases, component failures will cause only slight degradations. A total failure of the subsystem is extremely unlikely. Consequently failures of the subsystem are defined in terms of the degrees of degradation, based entirely on judgment. These failure definitions are briefly summarized as follows:

For the Control Room: (1) loss of more than half of the control-room CRTs with the wall diagram up, or loss of more than a quarter of the CRTs with the wall diagram down; (2) Loss of 2 or more keyboards in the control room.

For Shift Support and Software Maintenance and Development: Loss of 30% or more of the installed facilities for the function.

Because of the extremely low likelihood of losing a large number of CRTs or display generators, the exact probabilities of such events were not calculated in the reliability analysis. Instead, conservative approximations were made to simplify the computations of the reliability indices of the MMS subsystem. These indices are summarized in Table 5 .

TABLE 5

Man-Machine Subsystem Reliability Indices

Function	Failure Freq., per yr.	Availability
Control room	0.049	0.999997
Shift Support	0.130	0.999992
Software M & D	0.343	0.999980

Note that the frequencies of failure in the above Table are computed from the unavailabilities and a replacement time (by a spare component on the shelf) of 0.5 hour. A more detailed description of the reliability computations of the MMS is given in Appendix C.

5. SCC FUNCTION RELIABILITY

The probabilities of successfully carrying out specified functions using the DACS facilities at SCC are referred to as the reliabilities of the SCC functions. The reliability index of a given SCC function is computed by considering the subsystems needed for this function to be in a series configuration. The following list of SCC functions were considered:

(1) Real-time monitoring of the bulk electricity system (BES).
(2) Security and deployment of the BES.
(3) Study and forecast of the BES.
(4) Off-shift support in BES operations.
(5) Quality Assurance of software (S/W) for BES operations.
(6) Development of S/W for BES operations.

The block diagrams in Figure 8 show the subsystems needed in performing the above functions. In actual computations of the SCC function reliabilities, only the relevent segments of some of the subsystems need to be included. These segments of the subsystems are given in Appendix D.

The results of the reliability computations are given in Table 6.

TABLE 6

Reliability of SCC Functions

Function	Avail.	Outage Freq., 1/yr	MTTR min.
R/T monitoring of BES	0.9998909	48.078	1.192
Security & deploy. of BES	0.9995420	135.632	1.775
Study & forecast of BES	0.9990470	159.379	3.143
Off-shift support in BES op.	0.9990424	159.460	3.156
QA of S/W for BES op.	0.9754776	33.126	389.090
Develop.of S/W for BES op.	0.9753927	33.270	388.742

6. CONCLUSION

A reliability assessment has been carried out for the DACS facilities to be installed at the new SCC. The assessment was carried out in two steps: (1) Reliability analysis of the subsystems of DACS, and (2) Computation of the reliability indices of the SCC functions. The results are presented in this report. The reliability targets wherever given are generally met.

It should be noted that outage data for some of the subsystem components are not readily available. In such cases reasonable values were used based on experience, engineering judgment and acceptability to the client. Conservative approximations were made in computing the reliability indices.

The subsystems of DACS are highly redundant by design, and consequently, the reliability indices for the SCC functions will not be very sensitive to outage data variations of subsystem components.

Approved

A.H. Chung
Manager
Operations Research Dept

Submitted

L. Wang
Senior Engineer-Reliability
Reliability and Statistics Section

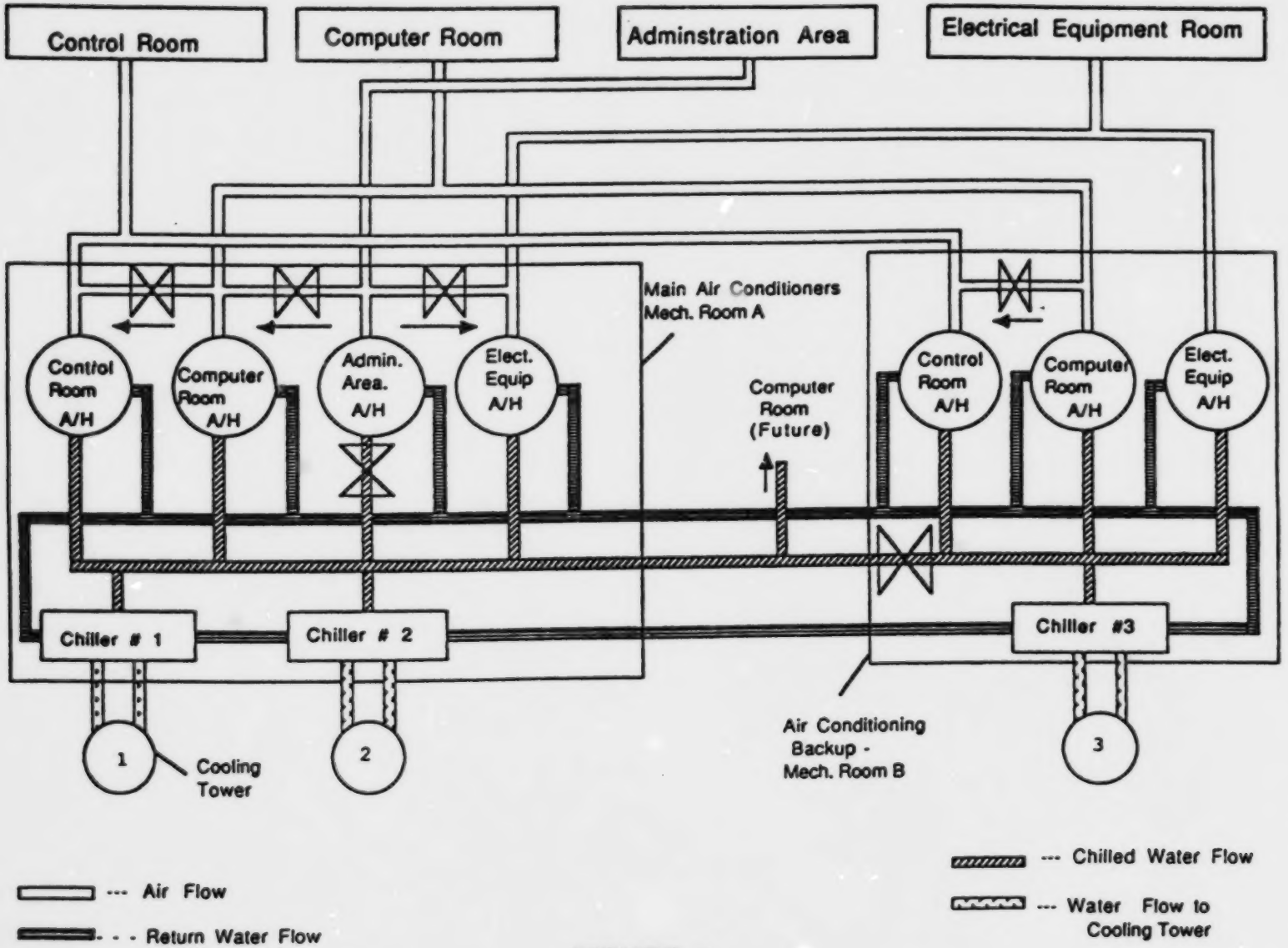


FIGURE 1
CLARKSON SCC HVAC SYSTEM

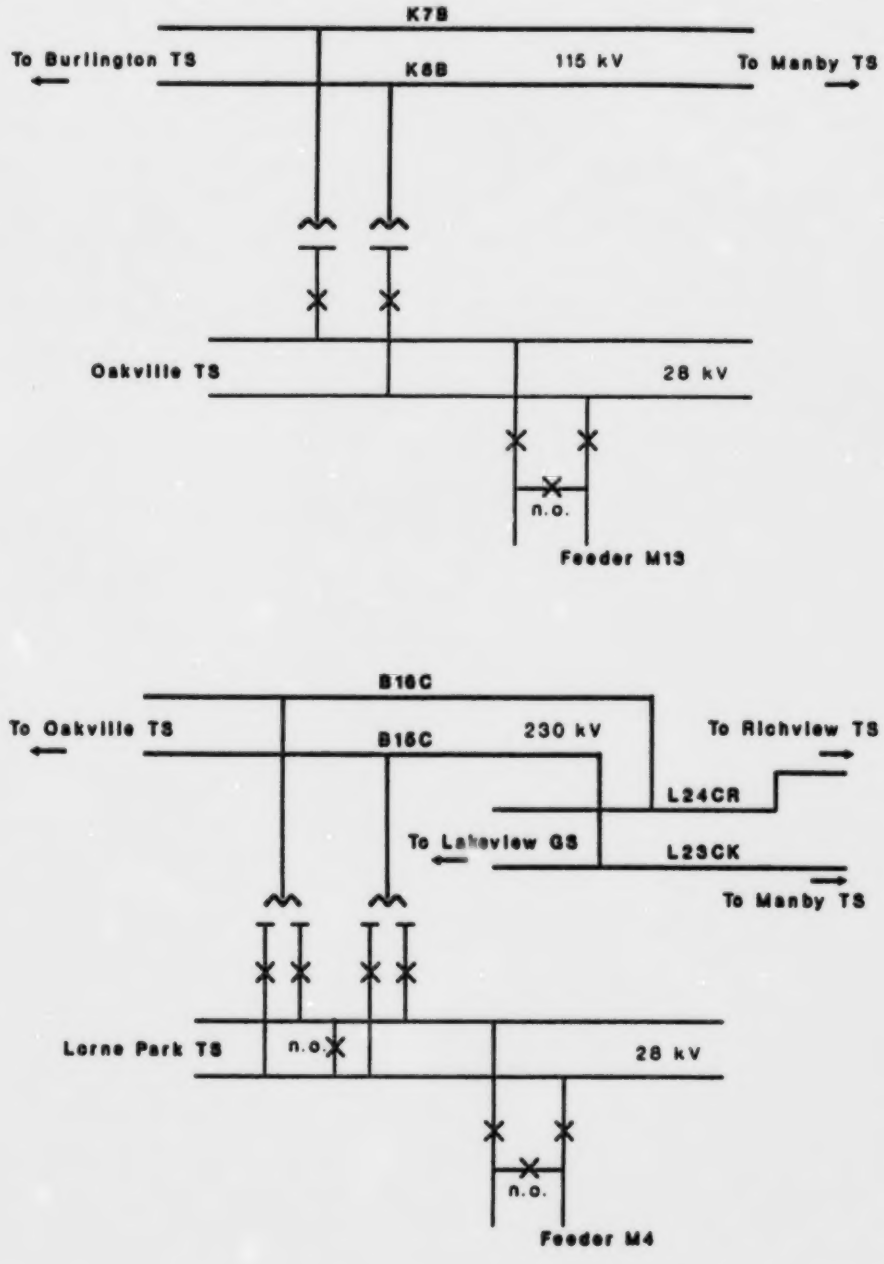


FIGURE 2
BES SUPPLY TO CLARKSON SCC

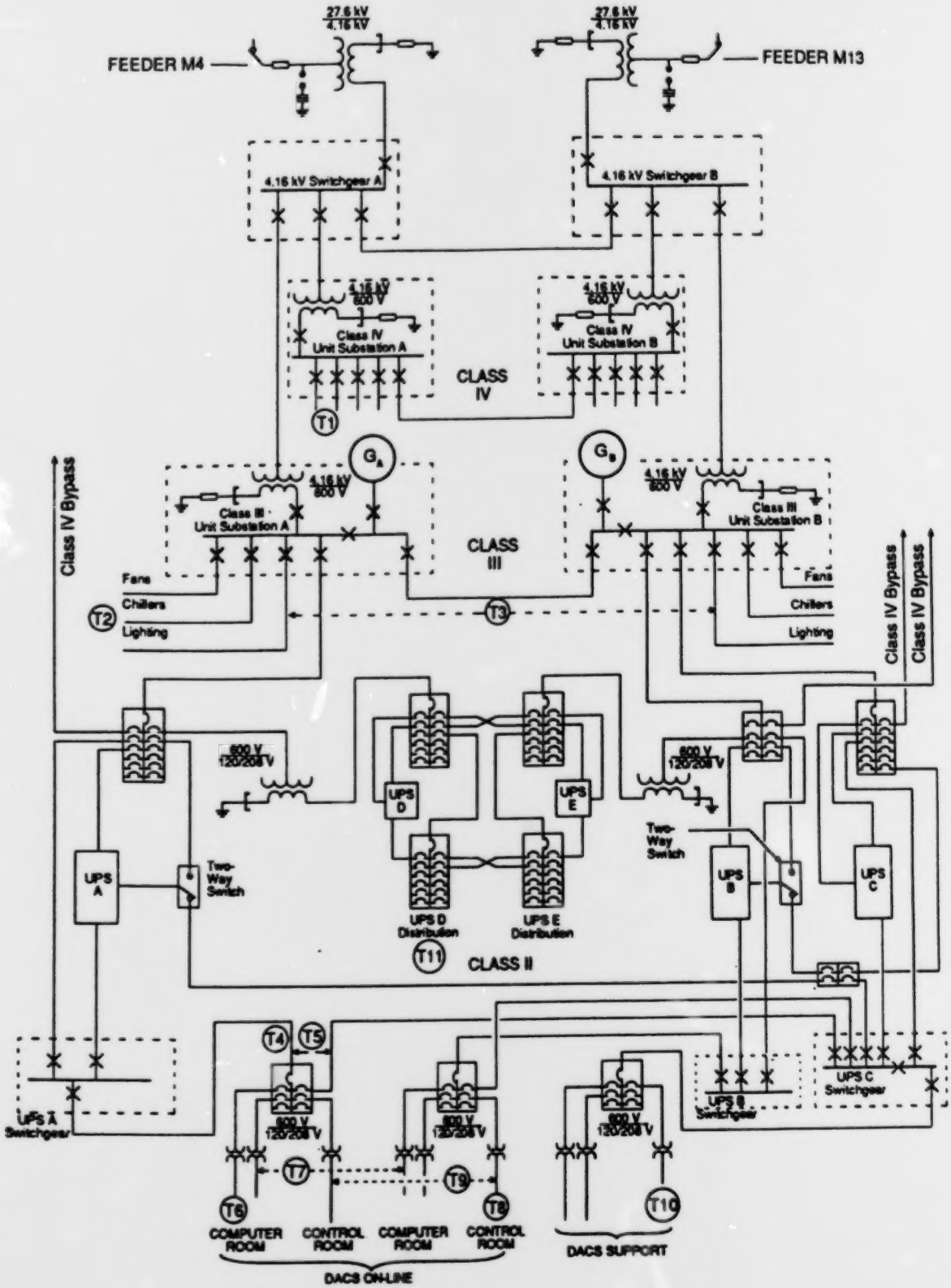


FIGURE 3
SCC POWER SUPPLY SUBSYSTEM

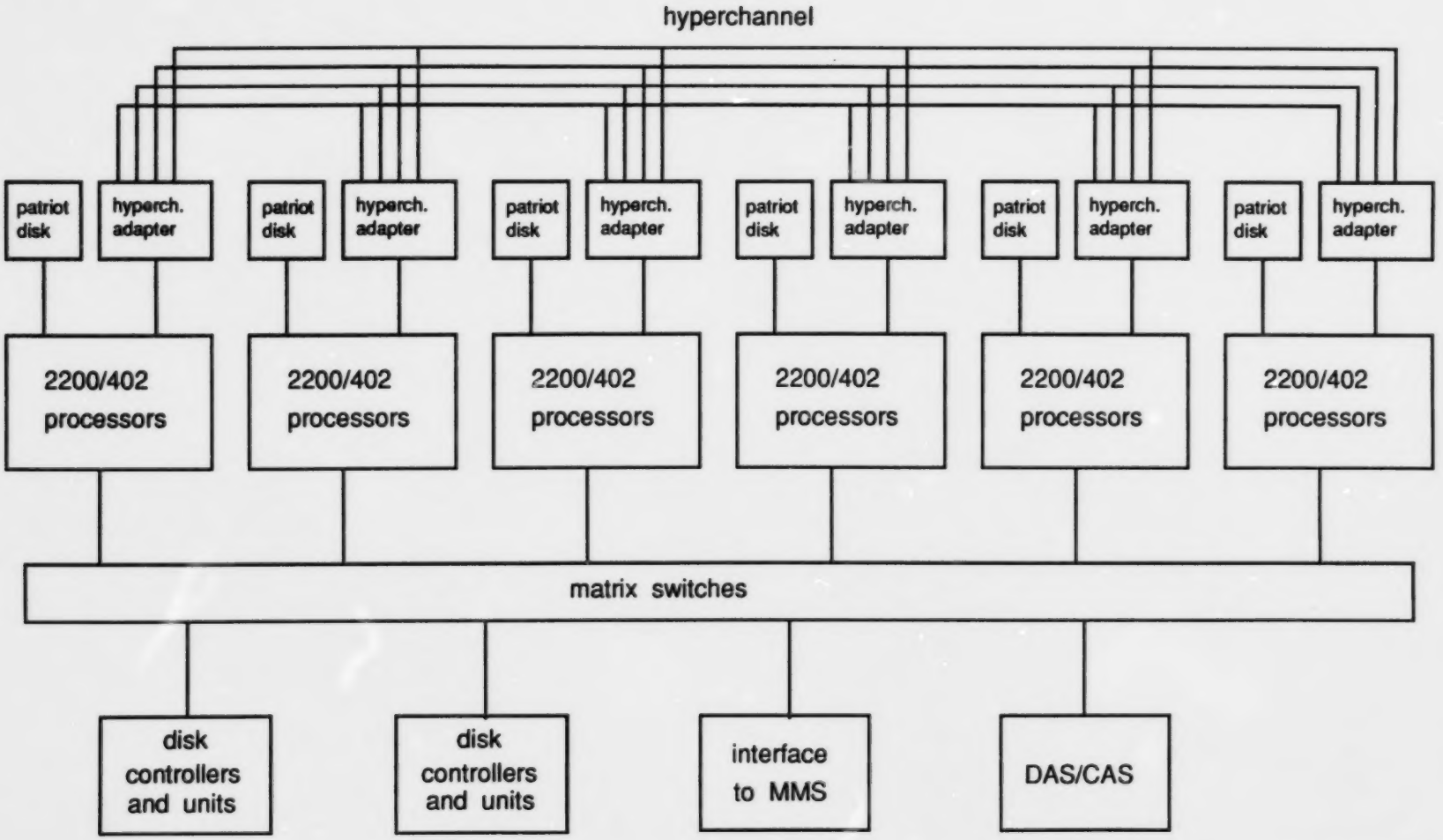


FIGURE 4
SIMPLIFIED BLOCK DIAGRAM PF 0N-LINE COMPUTER SUBSYSTEM

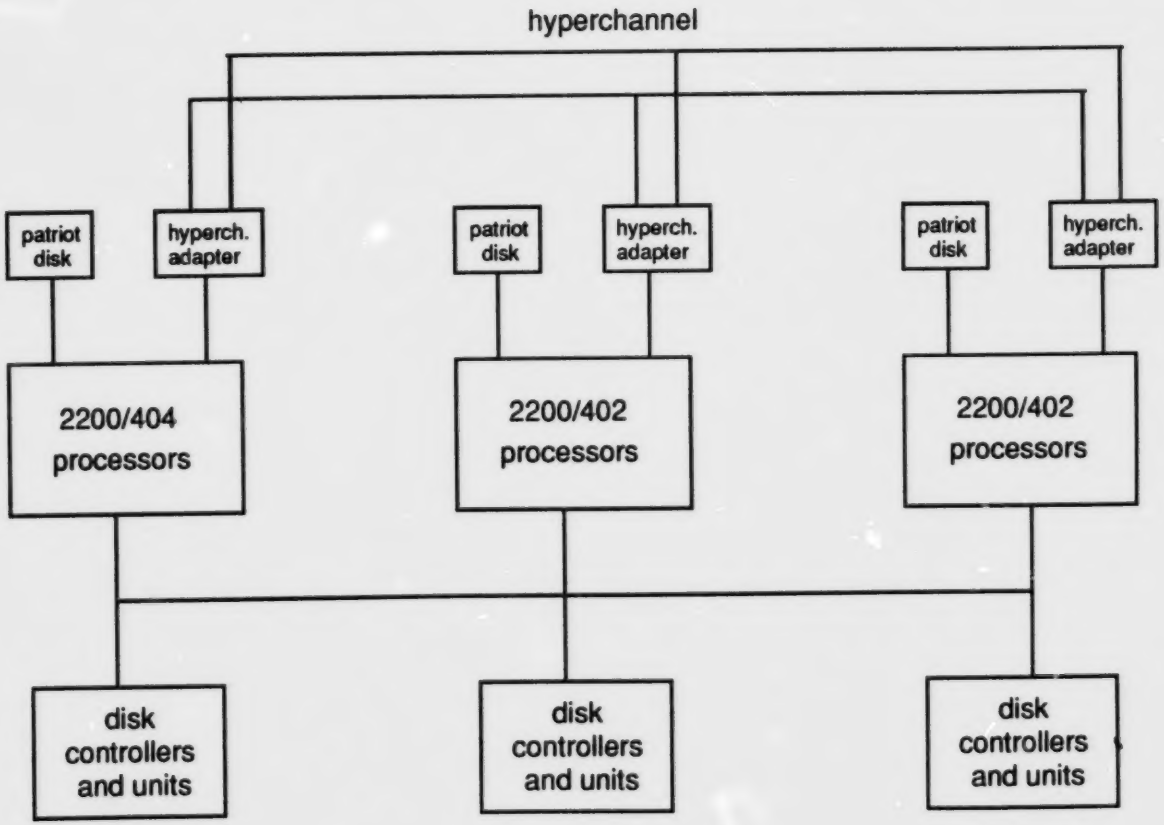


FIGURE 5
SIMPLIFIED BLOCK DIAGRAM OF COMPUTER SUBSYSTEM FOR SUPPORT FUNCTION

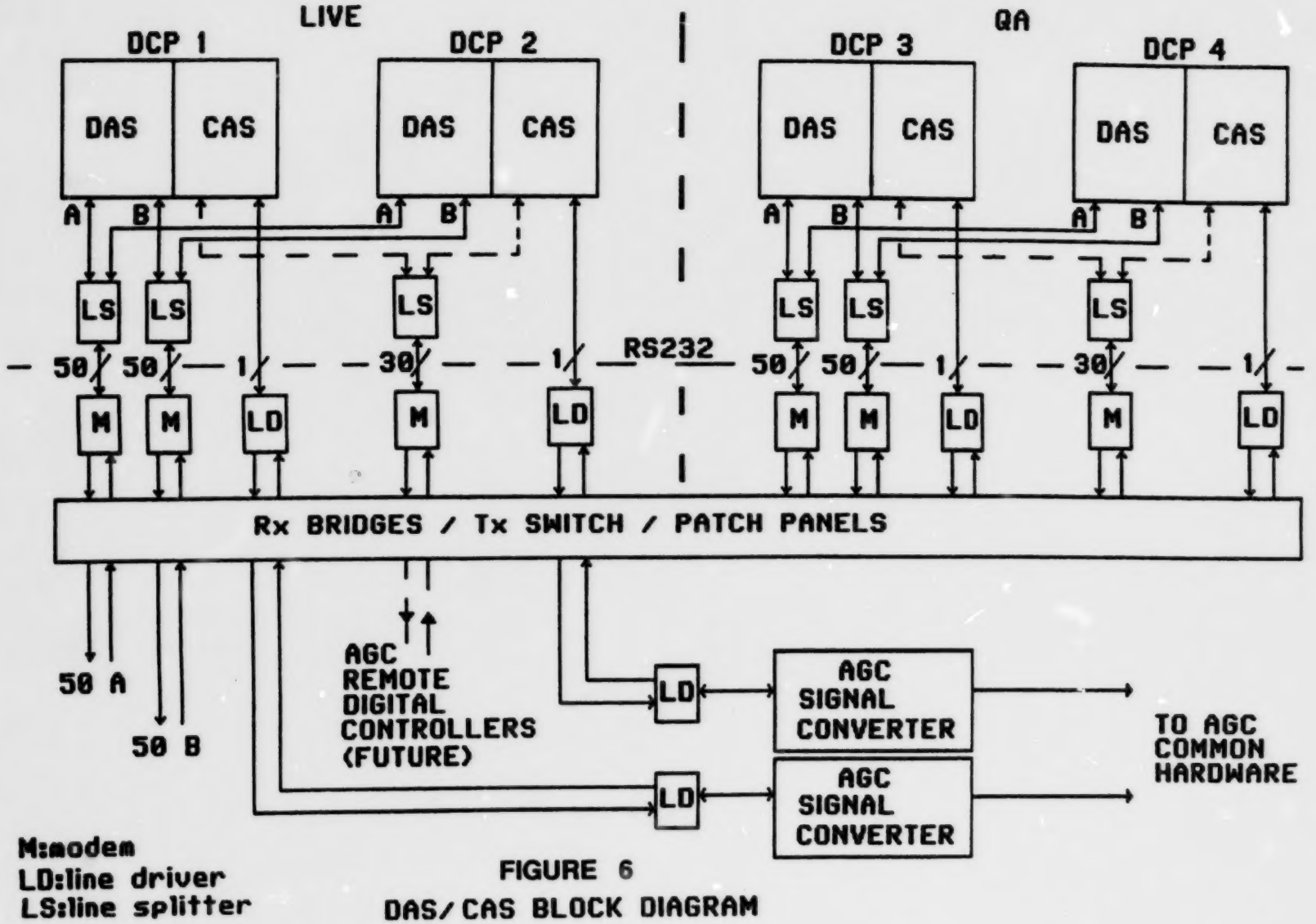


FIGURE 6

DAS/CAS BLOCK DIAGRAM

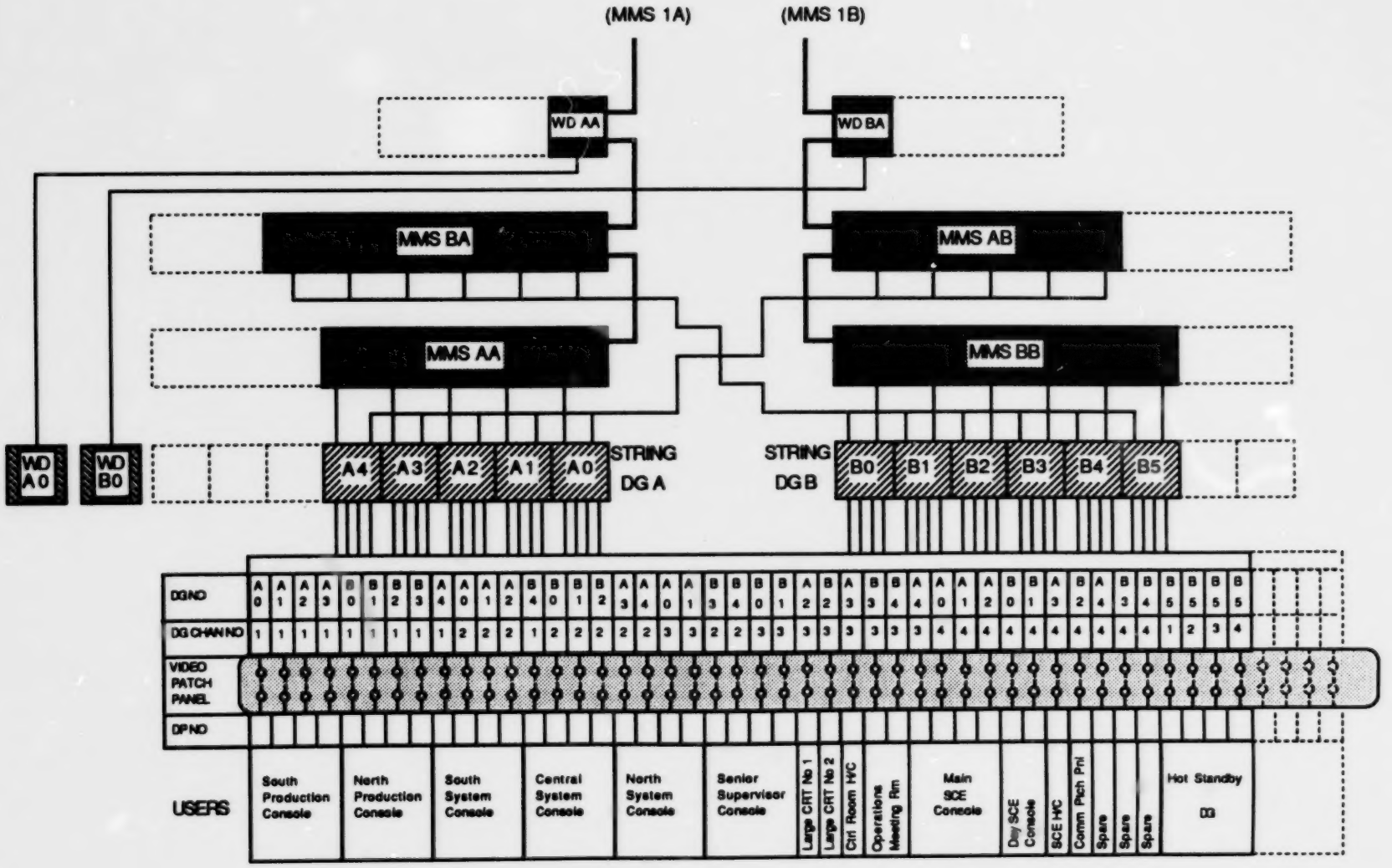
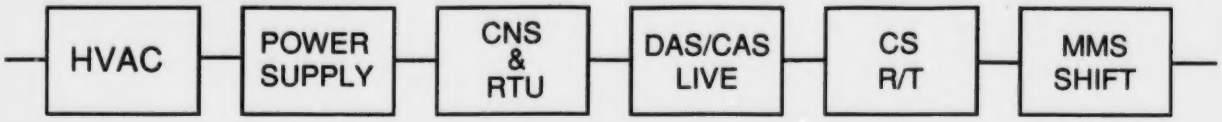
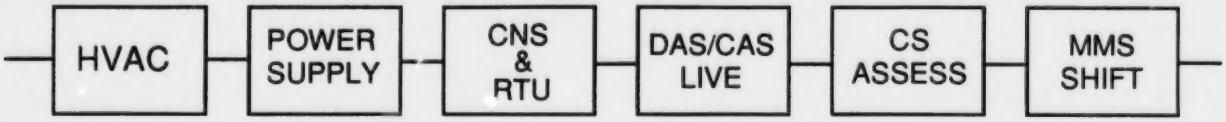


FIGURE 7
MMS BLOCK DIAGRAM - LIVE SYSTEM

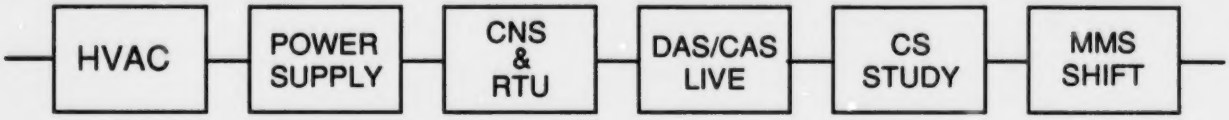
1. Real-time Monitoring of BES



2. Security and deployment of BES

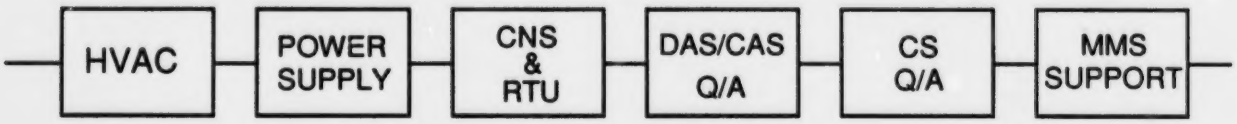


3. Study and Forecast of BES



4. Off-shift Support in BES Operations

5. Quality Assurance of Software for BES operations



6. Development of software for BES Operations

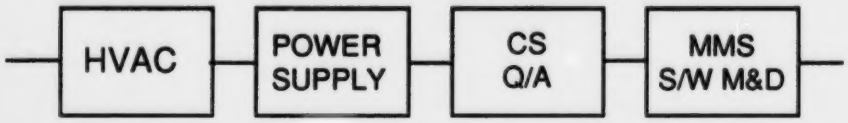


FIGURE 8
BLOCK DIAGRAM OF SCC FUNCTIONS

APPENDIX A

COMPUTER SUBSYSTEM RELIABILITY COMPUTATIONS

The reliability computations of the computer subsystem were carried out on an IBM compatible Personal Computer using LOTUS 1-2-3. This Appendix gives the input data, the details of the spreadsheet computations, and the appropriate assumptions for these computations. The details and assumptions are presented separately for the on-line, quality assurance, and support function computer subsystems.

A1. INPUT DATA

A1.1 Component Failure Data

Component	MTTF hrs	MTTR hrs
Main processor	8000	8
patriot disk	4000	8
Hyprchannel adapter	8000	0.5
Matrix switch	50000	0.5
Disk controller	8000	8
Disk unit in string	4000	8

A1.2 On-line Computer Subsystem Interruption Durations

Event	Duration, min
R/T node Auto-switchover time	1
Assessment node wait for R/T node	3
Full system recovery:	
R/T & Assessment nodes	5
Study node	8

A1.3 Planned Outages

On-line system	Duration	Freq 1/yr
R/T node	1 min.	24
Assessment node	1 min.	64
Study node	1 min.	64
A or S node wait for R/T	3 min.	
Support function system		
R/T node	5 min.	24
Assessment node	4 hrs.	64
Study node	4 hrs.	64
A or S node wait for R/T	8 min.	

A1.4 Software Failures

On-line system	Dur. min.	Freq 1/yr
R/T node	1	18
Assessment node	1	18
Study node	1	18
Support function system		
R/T node	5	18
Assessment node	5	18
Study node	5	18

A2. ON-LINE COMPUTER SUBSYSTEM RELIABILITY COMPUTATIONS

A2.1 Real-time Monitoring

System State	Unavail.	Freq.	Avail.
a. 0-1 Minute Failures			
R/T node	8.33E-06	4.38	
Hyperch.adapter	2.08E-06	1.095	
Matrix switch	3.33E-07	0.1752	
> 2 disk controller fail.	1.25E-11	0.000006	
Disk string failure	4.67E-07	0.24528	
Software	0.000034	18	
Subtotal	0.000045	23.89548	
b. 1-5 Minute Failures			
R/T+1 LIVE nodes	1.39E-10	0.000024	
2 consec. R/T node failure	1.76E-10	0.000030	
Subtotal	3.15E-10	0.000055	
c. 5-15 Minute Failures	0	0	
d. Planned Outages (1 min.)	0.000045	24	
R/T Node, total	0.000091	47.89554	0.999908

A2.2 Sscurity Assessment

System State	Unavail.	Freq.	Avail.
a. 0-1 Minute Failures			
Assessment node	8.33E-06	4.38	
Hyperchannel adapter	2.08E-06	1.095	
Matrix switch	3.33E-07	0.1752	
Software failure	0.000034	18	
Subtotal	0.000044	23.6502	
b. 1-5 Minute Failures			
R/T node failure	0.000136	23.89554	
2 consec. Asses. node fail.	1.8E-10	0.000030	
Asses. + study nodes	6.9E-11	0.000012	
Subtotal	0.000136	23.89558	
c. 5-15 Minute Failures	0	0	
d. Planned Outages			
R/T node (3 min.)	0.000136	24	
Assessment node (1 min.)	0.000121	64	
Subtotal	0.000258	88	
Assessment Node, total	0.000440	135.5457	0.999559

A2.3 Study and Forecast

System State	Unavail.	Freq.	Avail.
a. 0-1 Minute Failures			
Software failure	3.42E-05	18	
b. 5-Minute Failures (full system recovery)			
Study node failure	4.17E-05	4.38	
Hyperchannel adapter	1.04E-05	1.095	
Matrix switch	1.67E-06	0.1752	
Assess. node (0-1 min. f.)	0.000224	23.6502	
Subtotal	0.000278	29.3004	
c. 5-15 Minute Failures			
R/T node failure	0.000363	23.89554	
Assess.node (1-5 min. f.)	4.69E-10	0.000030	
R/T+assess. nodes	6.94E-11	0.000004	
Subtotal	0.000363	23.89557	
d. Planned Outages			
R/T node (3 min.)	0.000136	24	
Study node (1 min.)	0.000121	64	
Subtotal	0.000258	88	
Study Node, total	0.000935	159.1959	0.999064

A2.4 On-line Computer Subsystem Outages due to Disk Unit Failures

An outage of 1.5 hours will occur to the real-time (R/T) node when a LIVE disk unit and its backup in the second disk string develop overlapping failures in the LIVE system. The indices for such an event is computed as follows:

The R/T node operates in a degraded state when a LIVE disk unit has failed and the spare disk unit in the same string is in the process of being brought up (in 30 min.).

Probability [R/T node in a degraded state]
= 0.000125

Probability [R/T node in full outage due to overlapping disk failures]
= 3.28E-07

Frequency of full outages of the R/T node due to overlapping disk failures
= 0.001916 (per year, or once every 522 years)

A3. COMPUTER SUBSYSTEM FOR QUALITY ASSURANCE

A3.1 Assumptions:

(1) The quality assurance (QA) group is defined as failed if one or more of its three nodes becomes inoperative. Any failure which requires a LIVE node to be replacement by a QA node will result in the failure of the QA group.

(2) Software failures and planned outages in the LIVE group normally do not require reconfiguration of the computer nodes, and therefore do not cause QA failure.

(3) Software failures and planned outages in QA is not considered as failures of the QA group.

(4) The minimal-cut approximation is applied in the calculations. Only single and double contingency hardware failures are considered.

(5) Repairs of the failed hardware components are needed to restore the QA group to the up state.

A3.2 Reliability Computations for Computer Subsystem for QA

System State	Unavail.	Freq.	Avail.
Any 1 of the 6 on-line nodes	0.024	26.28	
Hyperchannel adapter	0.000375	6.57	
Disk unit failures	0.000125	0.001916	
QA group, total	0.0245	32.85191	0.9755

A4. COMPUTER SUBSYSTEM FOR SUPPORT FUNCTIONS

A4.1 Assumptions

(1) Two DCP's are included in the reliability assessment. Only one is required in normal operations.

(2) There are 4 processors in the R/T node, and 2 each in the Assessment and Study nodes.

(3) No fail-over of the R/T node to the Assessment and Study nodes can take place in the computer subsystem for support functions. The R/T node can function in degraded states with 2 or more of its 4 processors operating. The node is considered failed if more than 2 processors are down.

(4) No fail-over of the Assessment node to the Study node can take place because of differences in their peripherals (e.g., the number of disks in the disk strings).

(5) It takes 5 minutes to recover from a software failure in any one of the 3 nodes.

(6) The number of software failures in the computer subsystem for support functions is the sameas in the on-line system.

(7) All hardware failures in the Assessment or Study node result in full outages of the node. The failed node is returned to service at the completion of a repair.

(8) The number of planned outages in the support function system is the same as in the on-line system. The duration of a planned outage of the R/T node is 5 minutes. The duration of planned outages of the Assessment or Study node is 4 hours.

(9) Overlapping failures of 3 or more hardware components are assumed to be negligible.

A4.2 Reliability Computations for Computer Subsystem for Support Function - Real-time Node

System State	Unavail.	Freq.	Avail.
a. 5-Minute Failures			
Software failure	0.000171	18	
b. Full System Failures			
R/T node fail.	0.002006	2.19657	
Hyperchannel adapter	6.25E-05	1.095	
Both disk controllers	1.00E-06	0.001095	
Disk string failure	2.24E-04	0.24528	
DCP failure	3.44E-07	0.018094	
Subtotal	0.002293	3.556039	
c. Planned Outages (5 min.)	0.000228	24	
R/T Node - Support, total	0.002693	45.55603	0.997306

A4.3 Reliability Computations for Computer Subsystem for Support Functions - Assessment Node

System State	Unavail.	Freq.	Avail.
a. 5-Minute Failures			
Software	0.000171	18	
b. Full system failures			
Assessment node	0.004	4.38	
Hyperchannel adapter	6.25E-05	1.095	
Both disk controllers	1.00E-06	0.001095	
Disk string	2.24E-04	0.24528	
Subtotal	0.004287	5.721375	
c. Planned Outages			
R/T node	0.000365	24	
Assessment node	0.029223	64	
Subtotal	0.029589	88	
Assessment - Support, total	0.034047	111.7213	0.965952

A4.4 Reliability Computations for Computer Subsystem for Support Functions - Study Node

System State	Unavail.	Freq.	Avail.
a. 5-Minute Failures			
Software	0.000171	18	
b. Full System Failures			
Study node	0.004	4.38	
Hyperchannel adapter	6.25E-05	1.095	
Both disk controllers	1.00E-06	0.001095	
Disk string	2.24E-04	0.24528	
Subtotal	0.004287	5.721375	
c. Planned Outages			
R/T node	0.000365	24	
Study node	0.029223	64	
Subtotal	0.029589	88	
Study Node - Support, total	0.034047	111.7213	0.965952

APPENDIX B

DAS/CAS SUBSYSTEM RELIABILITY COMPUTATIONS

Reliability computations for the DAS/CAS subsystem is also carried on an IBM compatible Personal Computer using LOTUS 1-2-3. This Appendix contains the input data and the details of the spreadsheet computations.

B1. INPUT DATA

B1.1 DAS/CAS Component Outage Data

Component	MTTF, hr	MTTR,hr
DCP	4380	8
LS	43800	0.5
Modem	17520	0.5

B1.2 Mean Repair Delays for Failures Outside Normal Working hours:

	hrs.
Failures on Weekdays - Short delay (SD)	8
Failures on Weekends - Long delay (LD)	32
Mean switchover time -- LIVE to QA	10 min.

B1.3 System Failure Definition - LIVE or QA

Loss of one or more of the A and the corresponding B paths simultaneously.

B1.4 Assumptions

(1) Repair work will start rightaway when a component fails during the normal working hours.

(2) When a component fails outside the normal working hours and the rest of the system are up, repairs will start on the next working day.

(3) Upon the occurrence of a second component failure, maintenance will be called in to start repair work.

(4) Manual switchover to the QA system will be made when the LIVE system has failed.

(5) Simultaneous failures of more than two components are assumed

to be negligible.

(6) The communications network is assumed to be perfectly reliable.

B2. RELIABILITY COMPUTATIONS

B2.1 DAS/CAS LIVE Reliability

1. QA fully functional Prob. = 0.866846

Failure event/LIVE	Prob.	Freq.	Avail.
Fst DCP fail., SD	0.007305		
Fst DCP fail., LD	0.018264		
Dble cont with SD	2.78E-07	0.014611	
Dble cont with LD	6.95E-07	0.036529	
Subtotal, DCP	3.97E-07	0.020874	0.999999
Fst LS/M fail, SD	0.067922		
Fst LS/M fail, LD	0.259703		
Dbl cont. LS/M, SD	9.05E-07	0.047545	
Dbl cont. LS/M, LD	3.46E-06	0.181792	
Subtotal, LS/M	1.42E-06	0.074463	0.999998

2. QA impaired Prob. = 0.133153

Failure event/LIVE	Prob.	Freq.	Avail.
Fst DCP fail.-LIVE	0.003652		
Dble cont./DCP-LIVE	3.34E-06	0.007305	
Subtotal, DCP	4.44E-07	0.000972	0.999999
Fst LS/M fail.-LIVE	0.003995		
Dbl cont LS/M,-LIVE	7.98E-08	0.002796	
Subtotal, LS/M	1.06E-08	0.000372	0.999999
DAS/CAS LIVE overall		0.096682	0.999997

B2.2 DAS/CAS QA reliability

Failure event	Prob.	Freq.	Avail.
Fst DCP fail., SD	0.007305		
Fst DCP fail., LD	0.018264		
Dble cont with SD	2.78E-07	0.014611	
Dble cont with LD	6.95E-07	0.036529	
Subtotal, DCP	3.97E-07	0.020874	0.999999
Fst LS/M fail, SD	0.067922		
Fst LS/M fail, LD	0.259703		
Dbl cont. LS/M, SD	9.05E-07	0.047545	
Dbl cont. LS/M, LD	3.46E-06	0.181792	
Subtotal, LS/M	1.63E-06	0.085901	0.999998
DAS/CAS QA overall		0.106775	0.999997

APPENDIX C

MAN-MACHINE SUBSYSTEM RELIABILITY COMPUTATIONS

The man-machine subsystem consists of devices for inputting control commands (keyboards) and devices for displaying the status of the power system (CRTs, wall diagram). The redundancies are high and component failures will cause only slight degradations in most cases. Included in this Appendix are the input data and the reliability computations on an IBM compatible Personal Computer using LOTUS 1-2-3.

C1. INPUT DATA

C1.1 MMS Component Outage Data

Component	MTTF hrs.	Replacement Time, hrs.	MTTR hrs.
CRT	4800	0.5	8
Display gen.	4000	0.5	8
I/F unit	5000	0.5	4
Key board	8000	0.25	4
DMUX	8000	0.5	4
DCU	8000	0.5	4

C1.2 Control Room Facilities

24 CRTs on-line, 1 on-the-shelf spare.
9 display gen. on-line, 1 on-the-shelf spare.
6 keyboards, 1 spare.
1 wall diagram.

C1.3 System Failure Definition - Control Room

(1) Loss of more than half of the CRT's in the control room with the wall diagram up.

(2) Loss of more than a quarter of the CRT's in the control room with the wall diagram down.

(3) Loss of 2 or more keyboards in the control room.

C1.4 Shift Support Facilities

24 CRT's, 1 spare.
7 display generators, 1 spare.
12 keyboards, 1 spare.

C1.5 System Failure Definition - Shift Support

Loss of 30% or more of the facilities for the shift supprot function.

C1.6 Software Maintenance and Development Facilities

24 CRT's, 1 spare.
8 display generators, 1 spare.
14 keyboards, 1 spare.

C1.7 System Failure Definition - Software Maintenance and Development

Loss of 30% or more of the facilities for the function.

C2. RELIABILITY COMPUTATIONS

C2.1 Man-machine Subsystem - Control Room and Shift Control Engineer

Event	Prob.	Freq.	Avail.
CRT's			
All CRTs up	0.962261		
1 CRT down	0.037048	42.14703	
2 CRTs down	0.000682	1.555110	
3 CRTs down	8.00E-06	0.027396	
More than 20 CRTs up			0.999999
Display Generators			
All display gen up	0.982020		
1 dispaly gen down	0.017834	21.50625	
2 display gen down	0.000144	0.351519	
3 display gen down	6.82E-07	0.002526	
More than 6 DGs up			0.999999
Interface Units			
Both I/F units up	0.999100		
1 I/F unit down	0.000899	3.500846	
At least 1 I/F up			0.999999
Keyboards			
All keyboards up	0.997471		
1 keyboard down	0.002526	6.553386	
2 keyboards down	7.98E-08	0.013830	
5 or more KBs up			0.999997
Wall Diagram			
Both DUMX up	0.999437		
1 DUMX down	0.000562	2.188768	
At least 1 DUMX up			0.999999
Both DCUs up	0.999437		
1 DCU down	0.000562	2.188768	
At least 1 DCU up			0.999999
Other wall dia. comp.		0 (negl.)	1
MMS - Control Room (approx.)	0.048836		0.999997

C2.2 Man-Machine Subsystem - Shift Support

Event	Prob.	Freq.	Avail.
CRT's			
More than 20 CRTs up			0.999999
Display Generators			
All DG's up	0.985960		
1 DG down	0.013954	15.11477	
2 DG's down	0.000084	0.183360	
5 or more DGs up			0.999999
Interface Units			
Both I/F units up	0.999100		
1 I/F unit down	0.000899	3.500846	
At least 1 I/F up			0.999999
Keyboards			
All keyboards up	0.995975		
1 keyboard down	0.004017	6.543561	
2 keyboards down	1.29E-07	0.021993	
7 or more KB's up			0.999993
MMS - Shift Support		0.129957	0.999992

C2.3 Man-Machine Subsystem - Software Maintenance & Development

Event	Prob.	Freq.	Avail.
CRT's			
More than 20 CRTs up			0.999999
Display Generators			
All display gen up	0.983988		
1 dispaly gen down	0.015898	17.23947	
2 display gen down	0.000112	0.243722	
3 display gen down	4.57E-07	0.001479	
6 or more DG's up			0.999999
Interface Units			
Both I/F units up	0.999100		
1 I/F unit down	0.000899	3.500846	
At least 1 I/F up			0.999999
Keyboards			
All keyboards up	0.993488		
1 keyboard down	0.006491	6.527218	
2 keyboards down	2.13E-07	0.035543	
9 or more KB's up			0.999980
MMS - Software Main. & Dev.	0.342795		0.999980

APPENDIX D

SCC FUNCTION RELIABILITY COMPUTATIONS

As mentioned before, the reliability of a given SCC function is computed by considering the relevent segments of the subsystems needed for this function to be in a series configuration. Included in this Appendix are: (1) the reliability indices of the segments of the subsystems needed for the reliability computatoins, and (2) the computed relibility indices of six SCC functions.

D1. SUBSYSTEM RELIABILITY

Segment of Subsystem	Unavailability	Freqquency, 1/yr.
HVAC, Chilled water	1.090E-06	0.00452
Air-handling, Computer Rm.	3.924E-06	0.01088
Air-handling, Equip. Rm.	3.924E-06	0.01088
Air-handling, Control Rm.	3.924E-06	0.01088
Power supply at T1	7.850E-05	0.46948
Power supply at T2	4.390E-06	0.004808
Power supply at T3	2.020E-09	0.000005
Power supply at T4	1.150E-05	0.013263
Power supply at T5	2.670E-07	0.01328
Power supply at T6	7.980E-05	0.054645
Power supply at T7	8.540E-10	0.0000002
Power supply at T8	4.130E-05	0.041841
Power supply at T9	4.290E-10	0.0000001
Power supply at T10	7.480E-05	0.038462
Power supply at T11	4.490E-06	0.008475
On-line CS for R/T	9.110E-05	47.8955
On-line CS for Assessment	4.400E-04	135.5457
On-line CS for Study	9.350E-04	159.1959
On-line CS for QA	2.450E-02	32.8519
Support CS for R/T	2.693E-03	45.556
Support CS for Assessment	3.405E-02	111.7213
Support CS for Study	3.405E-02	111.7213
DAS/CAS Live	2.269E-06	0.096682
DAS/CAS QA	2.031E-06	0.106775
MMS - Control Room	2.788E-06	0.048837
MMS - Shift Support	7.418E-06	0.129958
MMS - Software M&D	1.957E-05	0.342795

D2. COMPUTATION OF SCC FUNCTION RELIBILITY

Function	Avail	Outage Freq. 1/yr	MTTR min
R/T monitoring of BES	0.9998909	48.0781793	1.1918221
Security & deploy. of BES	0.9995420	135.6316973	1.7745297
Study & forecast of BES	0.9990470	159.3785793	3.1425457
Off-shift support in BES op.	0.9990424	159.4597003	3.1562088
QA of S/W for BES op.	0.9754776	33.1257933	389.09037
Develop. of S/W for BES op.	0.9753927	33.270317	388.74168

ATTACHMENT 1

Reliability Assessment of the HVAC Systen for the Clarkson System Control Center

by
L. Wang

Research Division Report No. 88-219-K
September 27,1988

91602
new 82-10

ontario hydro
research division

To: Mr. R.C. Seaton
Project Manager
System Control Center Relocation Project
Design and Development-Transmission Division

RELIABILITY ASSESSMENT OF THE HVAC SYSTEM FOR THE CLARKSON SYSTEM CONTROL CENTER

L. Wang
Senior Engineer-Reliability
Reliability and Statistics Section
Operations Research Department

A reliability assessment was carried out for the heating, ventilating and air-conditioning system to be installed at the new System Control Center at Clarkson. The predicted unavailabilities and mean times between failures for the critical load areas are within the specified reliability targets. The computed mean downtimes for the computer room and the electrical equipment room are longer than the target value of 0.5 hour, which may not be attainable for a practical HVAC system.

1. INTRODUCTION

The new System Control Center (SCC) will be housed in a three-story building under construction at Clarkson. The continuous operation of the equipment in the new SCC requires a dependable air-conditioning system to provide a favorable operating environment. The heating, ventilating and air-conditioning (HVAC) system for the new SCC is designed with a high degree of redundancy to fulfill this requirement.

At the request of the System Control Center Relocation Project Department, a reliability assessment of the HVAC system for the new SCC was carried out. This report summarizes the results of this assessment.

2. SUMMARY OF RESULTS

The predicted unavailabilities, the mean times between failures (MTBF) and the mean down times of the air conditioning systems for the four load areas of the new SCC are given in Table 1, with the reliability targets given in brackets following the computed indices. Details of the computations are given in the Appendix.

job	file	date	report no.
72-212-422	813.07	September 27, 1988	88-219-K

The results in Table 1 show that the unavailability and the MTBF indices for the essential load areas (the control room, the computer room, and the electrical equipment room) are well within the specified reliability requirements. The mean down times of air-conditioning systems for the computer room and the electrical equipment room are longer than the specified values. An air-conditioning system failure in an essential load area can occur only when several components in the HVAC system fail simultaneously, exhausting all redundancies in the system. In such a case air-conditioning service can be restored only by completing the repair work of at least one of the failed components. It is unlikely that the mean repair times of the HVAC system components can be reduced significantly. Hence the specified mean down time of 0.5 hour for the computer room and the electrical equipment room air-conditioning systems may prove to be difficult to meet.

TABLE 1

HVAC System Reliability Indices

Load area	Unavailability	MTBF, yr.	Mean down time, hr.
Control room	5.09E-6 (9.0E-5)	64 (5)	2.86 (4)
Computer room	5.09E-6 (5.7E-6)	64 (10)	2.86 (0.5)
Electrical equip rm	5.09E-6 (5.7E-6)	64 (10)	2.86 (0.5)
Admin area	0.83E-3 (-)	1.2 (-)	4.77 (-)

An interruption of power supply to the HVAC system would cause it to stop functioning. The probability of occurrence of this event is approximately 2.0E-9, with a mean downtime of 4.0 hours.

As mentioned before, the HVAC system for the new SCC is designed with a high degree of redundancy. An air-conditioning system composed of components identical to those in the HVAC system for the new SCC but with no redundancy has an unavailability of 2.91E-3 (equivalent to a failure frequency of 4.72 times per year and a mean down time of 5.41 hours). This simple example shows that the high reliability levels of the HVAC system for the new SCC are achieved through redundancy. Real-life experience tells us that most air-conditioning systems with no redundancies perform much more reliably than the one given in the above example. This suggests that the results obtained in this assessment are not overly optimistic.

Approved:

A. H. Chung
Manager
Operations Research Department

LW:cmh

Submitted:

L. Wang
Senior Engineer-Reliability
Reliability and Statistics Section

APPENDIX

1. SYSTEM DESCRIPTION

The HVAC system is designed to perform three major functions: heating, cooling and air handling. A simplified diagram of the HVAC system is given in Figure A.1. Cooling is provided by three open-drive centrifugal chiller units, any two of which will be capable of handling the full building load. Any one unit can be operated to provide adequate capacity for essential loads, including the control room, the computer room, and the electrical equipment room, and their supporting areas. Chilled water is circulated to the air handling units for air-conditioning in required areas.

Much of the heating energy requirement can be produced from recovering the heat rejected by the operating chillers. This heat is available at a low temperature. Four pipe fan coil systems will be provided for perimeter space heating. Other fan coil heaters will also be provided in upper floor ceiling plenums and other areas requiring heating. A supplemental electric boiler will be installed to maintain heat recovery circuit temperatures during low internal load periods and to provide higher temperature water for entrance and bridge heating.

Duplicate central station air handling units will be provided for the three critical areas, including the control room, the computer room and the electrical equipment room. They will be installed in separate HVAC equipment rooms to provide standby capacity for each of the critical load areas in the event of equipment failure, maintenance, or even the destruction of one HVAC equipment room. The administration area will be serviced by a separate central station air handling unit located in the main HVAC equipment room.

A fixed amount of outside air will be supplied to all air handling unit, except the one for the administration area, at all seasons to ensure a constant quantity and quality of ventilation and to avoid potential freeze up problems associated with winter operation.

Since the air handling unit for the administration area may have different operating requirement, and is not considered an essential load, nor is it a large heat energy source, outside air economizer cooling will be provided to reduce winter refrigeration requirements. Operation of the chiller will not be required to provide cooling to the interior office spaces when outdoor ambient conditions allow direct use of outdoor air.

The air handling unit for the administration area is designated to serve as a backup for the units for both the computer room and the electrical equipment room. Backup for the control room air handling unit comes from those for the computer room.

An electronic control and monitoring system featuring distributed control, central monitoring and central control override will be provided to manage operating conditions. Automatic changeover from operating to standby equipment will be initiated in the event of a failure. Abnormal operating conditions will be alarmed to the central station. Provision will be made to communicate with an off-site monitoring facility through a telephone line.

2. FAILURES IN THE HVAC SYSTEM

In view of the designed redundancies in the HVAC system, failures of a single component may cause a temporary interruption of air-conditioning service to a particular load area. The duration of the temporary interruption is equal to the time required to complete an automatic or manual change-over operation. The durations of such temporary interruptions of air conditioning service are assumed to be sufficiently short so that they do not cause any problem in the operation of the SCC. Therefore, such temporary interruptions of air-conditioning service are not considered as system failures.

If no change-over operation can restore air-conditioning service, the system is considered failed.

The justifications for the definition of system failure stated above are based on the following considerations:

(1) the operation of the HVAC system is constantly monitored by an electronic monitoring system at two different locations in the SCC, and

(2) the operation of the electronic monitoring system can be tested at regular intervals to ensure that it functions normally.

Note that the above definition of system failure does not include any specification on the down time of the air-conditioning system. In reality, only air-conditioning system outages which last longer than a given length would affect the operation of the equipment in the SCC. Outages with downtimes shorter than this value are tolerable and technically they should not be classified as system failures. However, it is believed that only a small portion of air-conditioning system failures falls in this category, and the specification of a minimum downtime in the system failure definition would unnecessarily complicate the assessment process. Excluding the minimum downtime specification in the system failure definition results in lower reliability (or higher risk) indices for the air-conditioning systems.

3. METHOD OF ASSESSMENT

3.1 Assumptions

The following assumptions were made in this study:

- The electronic control and monitoring system is tested at regular intervals to ensure its proper functioning. This process reduces the probability of malfunctions in the HVAC system without being detected by the monitoring system or hidden failures of the monitoring system itself to a negligible level.

- At the detection of an abnormality in the HVAC system, manual change-over operations can be completed in a short time without causing difficulties in the operation of the SCC.

- The air-conditioning systems for the control room, the computer room, and the electrical equipment room operate in the cooling mode at all seasons. These systems are not affected by component failures in the heating subsystem.

- The air-conditioning system for the administration area operates in the cooling mode for two thirds of the year, and in the heating mode for the remainder of the time.

- The air handling unit for the administration area can backup the air handling units for the computer room, or those for the electrical equipment room, but not for both rooms at the same time.

- It may be possible to have free cooling utilizing outside air during the cool months. This mode of cooling operation can be applied to the administration area, the computer room, or the electrical equipment room. However, the effectiveness of this mode of operation is not certain, and therefore is not included in the reliability assessment.

- Component failures occur independently. Common-cause failures, such as those due to fire and earth-quake, are not included in the assessment.

- The effect of annual maintenance of the water chillers, fluid coolers, and air handling units are incorporated in the assessment. The duration of annual maintenance of the water chiller and fluid cooler combination is assumed to be one week, and that of the air handling unit is one day.

- Under normal conditions two chillers will be operated while the third will be placed on standby. The operating and the standby units will be rotated on a regular basis. The standby unit will undergo weekly start-up tests. The probability of occurrence of a start-up failure is assumed to be 0.05.

3.2 Logic Diagrams

In view of the designed redundancies in the HVAC system and the assumed independence of system components, the logic diagram approach seems to be the most suitable method for this study. A system represented by a logic diagram is considered working if there is a path between the input and output nodes of the diagram.

The HVAC system can be separated into three subsystems each of which performs one of the following three functions: cooling, air handling and heating. The logic diagrams for these subsystems are given in Figures A.2 to A.4. Note that the air handling subsystems for the different load areas in the SCC are not all identical. Backup air handling provisions for the essential load areas are indicated in the logic diagram in Figure A.3.

3.3 Assessment Procedure

The reliability of the air-conditioning system for each load area of the SCC is assessed separately. The seasonal operating modes of the air- conditioning systems are incorporated in the assessment.

The control room air-conditioning system is expected to operate in the cooling modes all year round. Its reliability indices can be calculated from the logic diagram of the chilled water subsystem in series with that for the appropriate air handling subsystem, with due consideration given to the availability of the backup arrangement.

The computer room and the electrical equipment room air-conditioning systems are also expected to operate in the cooling mode all the time. Their reliability indices can be calculated in a manner similar to that for the control room.

The administration area air-conditioning system is assumed to operate in the cooling mode for eight months in late spring,summer and fall, and in the heating mode for the remainder of the year. Reliability of the system in the cooling mode can be calculated from the logic diagrams of the chilled water subsystem and the appropriate air handling subsystem in series. In the heating mode, it can be calculated from the logic diagrams of the water heating and air handling subsystems in series. There is no backup arrangement for this system.

4. COMPONENT FAILURE DATA

No published failure data for air-conditioning system components were found in the literature. Failure data of similar components were used as references in selecting the failure rates and the mean repair times for these components. Both the reference data and the failure data used in this study are listed in Table A.1. In cases where no reference data could be found, suitable values were assumed based on judgement. The assumed failure data are believed to be conservative.

TABLE A.1

Component Failure Data

Component	Reported Data: Failure rate, /yr.	Reported Data: Mean Repair time, hrs.	Source*	Data used in study: Failure rate, /yr.	Data used in study: Mean repair time, hrs.
Chilled water pump	0.435	5.5	(1)	0.435	5.5
Flotrex disch. & bal. valve	0.083	3.7	(2)	0.083	3.7
Suction guide & strainer	0.019	10.0	(2)	0.019	10.0
Butterfly valve, manual	0.013	5.5	(2)	0.13	5.5
Condenser pump	0.435	5.5	(1)	0.435	5.5
Chiller/heat exchanger	0.041	24.0	(1)	0.2	24.0
Pneumatic valve	0.02	4.0	(2)	0.2	4.0
Pipe, 4-6", per meter	3.2E-6	-	(2)	3.2E-6	6.0
Temperature control valve	-	-	-	0.1	5.0
Diff. pressure bypass valve	0.074	7.6	(2)	0.074	7.6
Fluid cooler	-	-	-	0.1	5.0
Air handling unit	-	-	-	0.5	5.0
Dampers & controls	-	-	-	0.01	5.0
Ductwork	-	-	-	0.000876	5.0
Heating coil	0.0135	8.0	(2)	0.0135	8.0
Heat recovery pump	0.435	5.5	(1)	0.435	5.5
Electrical boiler	0.047	21.8	(1)	0.2	24.0
Hot water pump	0.435	5.5	(1)	0.435	5.5

* Source of data:

(1) Ontario Hydro Design and Development Division Report No. 76095, June, 1976.
(2) Ontario Hydro Design and Construction Branch Report No. 86296, Nov. 1986.

5. IMPACT OF REPAIR DELAYS

After the failure of a component in the air conditioning system, repair efforts could be delayed if the needed spare parts are not readily available. Such delays would adversely affect the reliability levels of the air-conditioning systems for the critical load areas in the new SCC. The impact on system reliability due to the lack of spare parts for one component may not be the same as that for another. It is useful to assess such impacts so as to determine the levels of spares needed for various key components in the HVAC system. Assessments were carried out by assuming 4-week delays in repairs following failures of some key components. The results of these assessments are given in Table A.2. Note that in these assessments the effect of repair delays in more than one type of component is not considered.

TABLE A.2

Impact of Repair Delays on HVAC Reliability for Critical loads

Component	Unavailability		MTBF, yrs.	
	Without delay	With delay	Without delay	With delay
Chilled water pump	5.09E-6	6.65E-6	64.2	62.1
Condenser pump	5.09E-6	6.65E-6	64.2	62.1
Chiller	5.09E-6	8.79E-6	64.2	63.0
Air handling unit	5.09E-6	51.6E-6	64.2	54.7

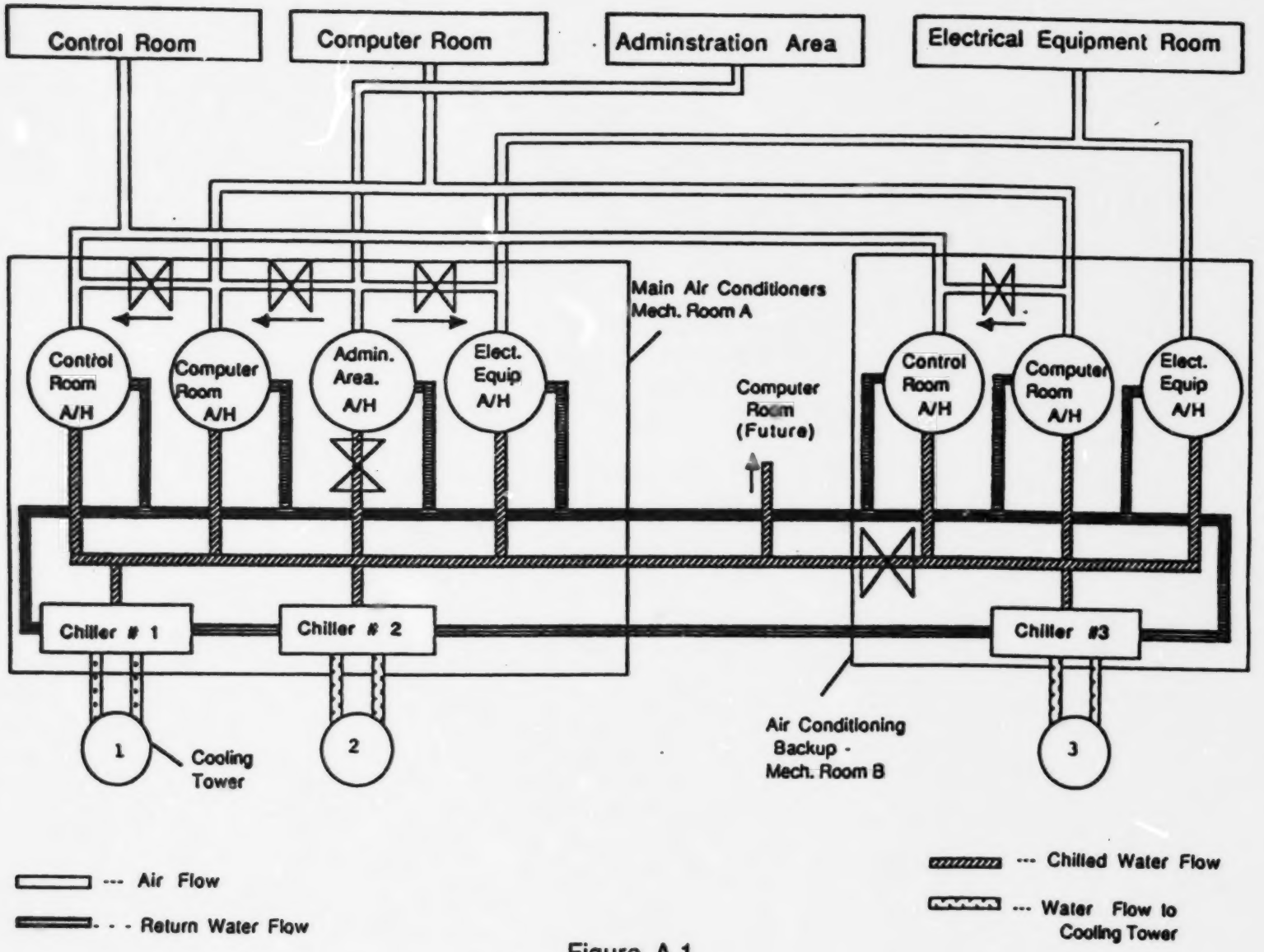


Figure A.1
Clarkson SCC HVAC System

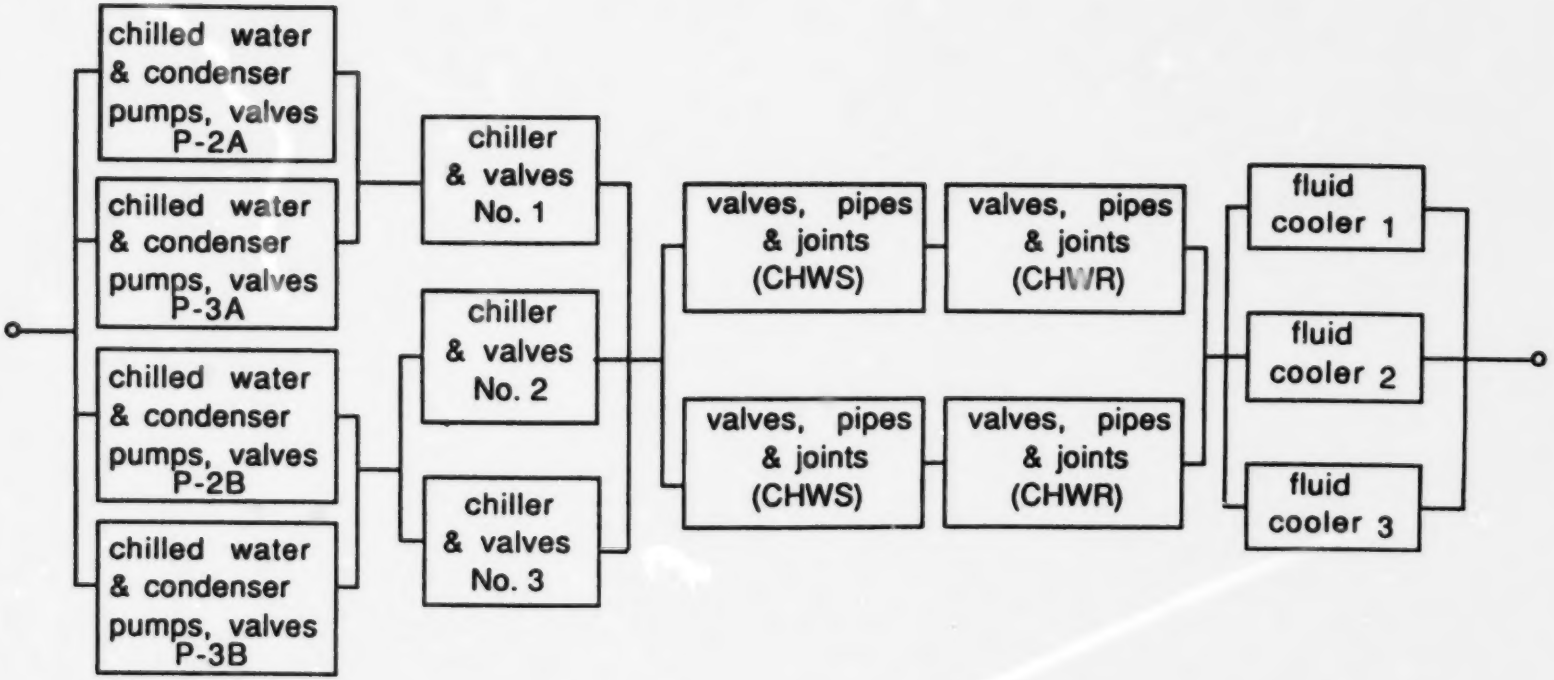

chilled water & condenser pumps, valves P-2A
chilled water & condenser pumps, valves P-3A
chilled water & condenser pumps, valves P-2B
chilled water & condenser pumps, valves P-3B
chiller & valves No. 1
chiller & valves No. 2
chiller & valves No. 3
valves, pipes & joints (CHWS)
valves, pipes & joints (CHWR)
valves, pipes & joints (CHWS)
valves, pipes & joints (CHWR)
fluid cooler 1
fluid cooler 2
fluid cooler 3

Figure A.2
Chilled Water Subsystem

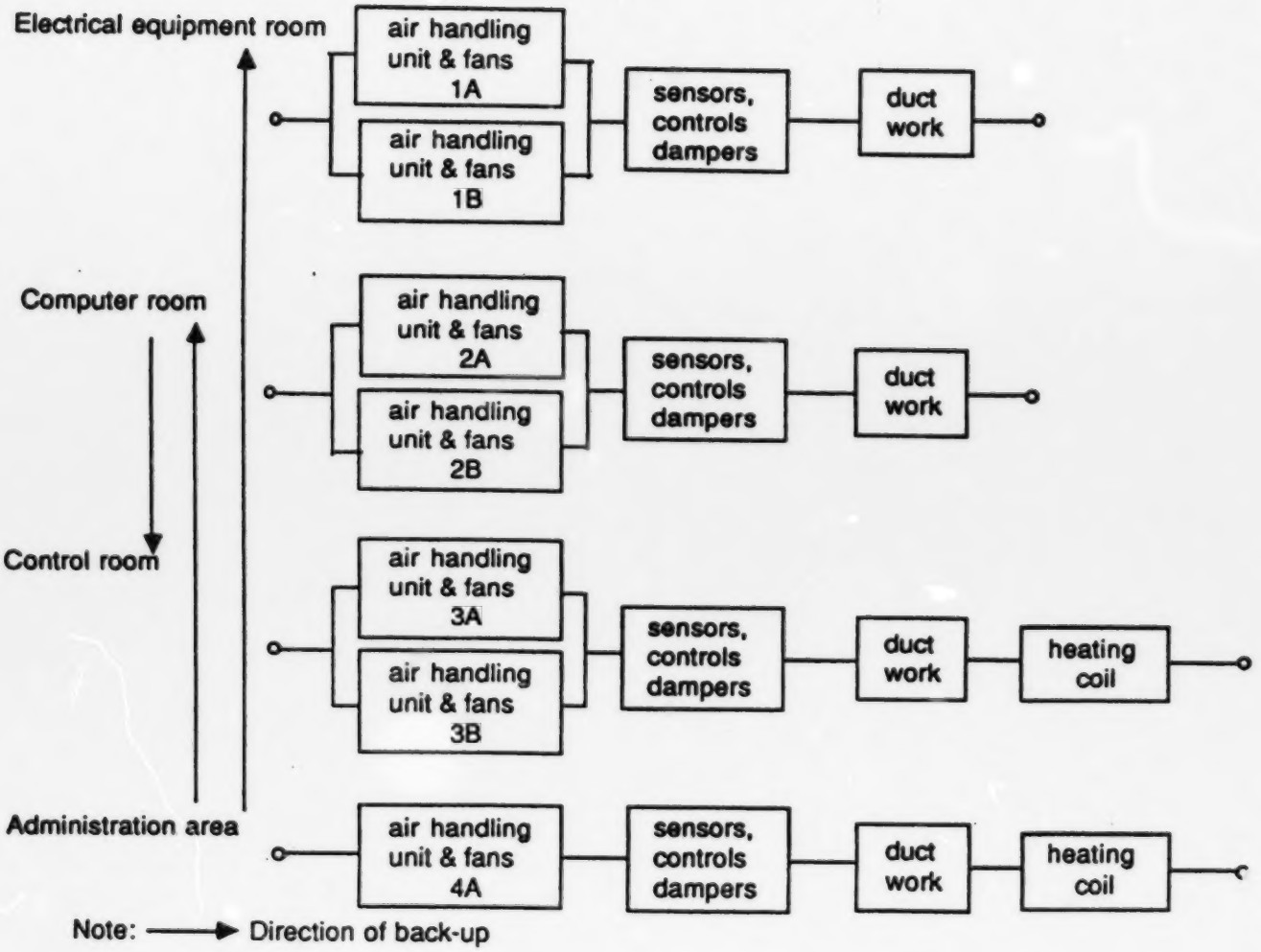


Figure A.3
Air Handling Subsystem

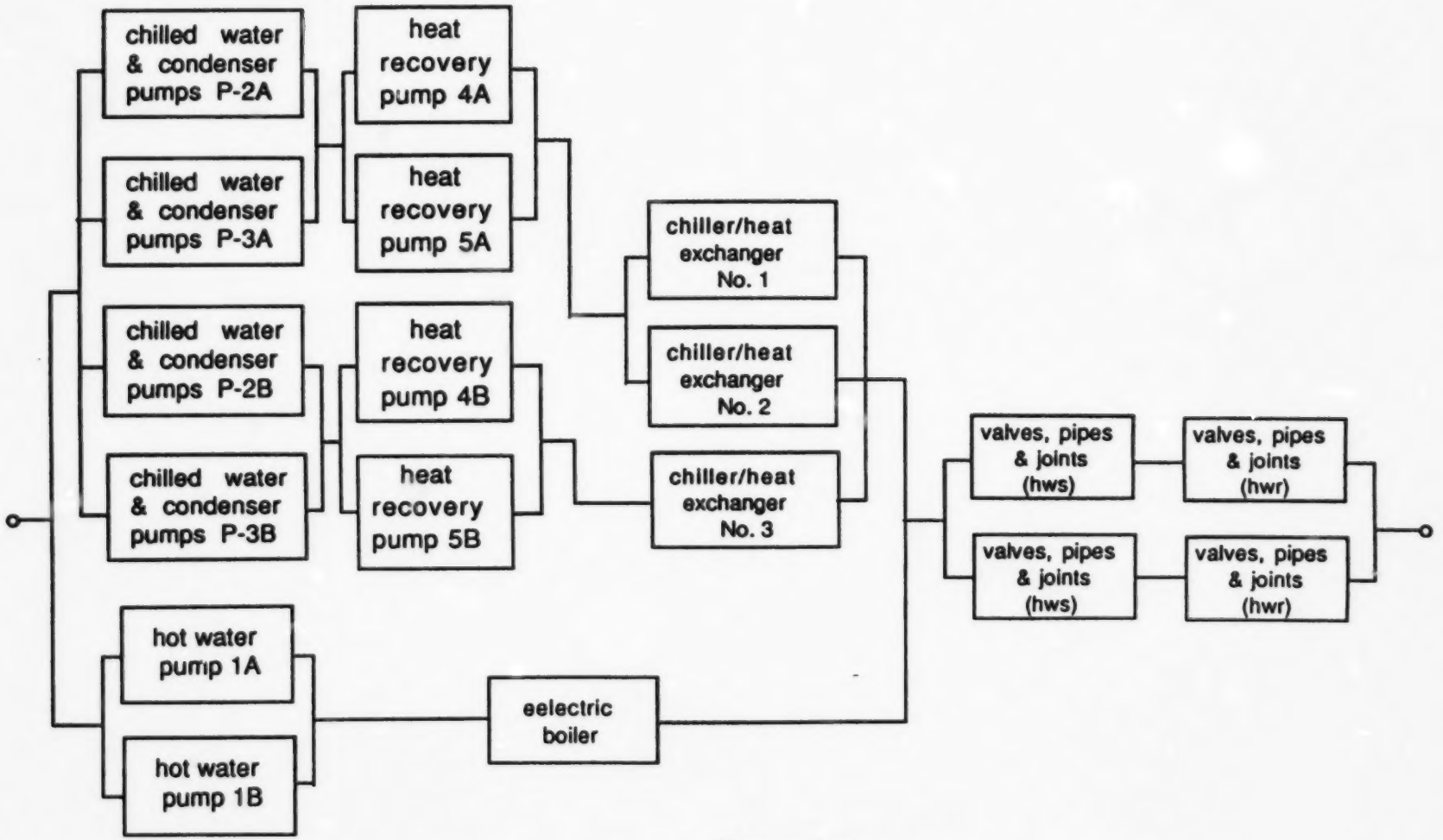

chilled water & condenser pumps P-2A
chilled water & condenser pumps P-3A
chilled water & condenser pumps P-2B
chilled water & condenser pumps P-3B
heat recovery pump 4A
heat recovery pump 5A
heat recovery pump 4B
heat recovery pump 5B
chiller/heat exchanger No. 1
chiller/heat exchanger No. 2
chiller/heat exchanger No. 3
valves, pipes & joints (hws)
valves, pipes & joints (hwr)
valves, pipes & joints (hws)
valves, pipes & joints (hwr)
hot water pump 1A
hot water pump 1B
eelectric boiler

Figure A.4
Water Heating Subsystem

ATTACHMENT 2

Reliability Assessment of the Power Supply for the Clarkson System Control Center

by
N. Ramani

Research Division Report No. 88-304-K
December 13,1988

91602
new 32-10

ontario hydro
research division

To: Mr. R.C. Seaton
Project Manager
System Control Center Relocation Project
Design and Development - Transmission Division

RELIABILITY ASSESSMENT OF THE POWER SUPPLY FOR THE CLARKSON SYSTEM CONTROL CENTER

Report No. 88-304-K

N. Ramani
Engineer
Reliability and Statistics Section
Operations Research Department

ABSTRACT

A reliability assessment of the power supply for the new system control center at Clarkson has been carried out. The mean times between failures, the mean times to restore service and the probabilities of interruption of power supply at various load points in the control center have been estimated and are used as the reliability indices. These values were examined by personnel from the relocation project team and judged to be acceptable.

1. INTRODUCTION

Ontario Hydro plans to move the System Control Center (SCC) to a new location at Clarkson by the year 1991. The Operations Research Department is taking part in the reliability evaluation of the new facilities. The current study forms a part of the investigation and examines the reliability of the power supply to the Control Center. This report summarizes the results of the assessment.

job	file	date	report no.
72-212-422	813.07		88-304-K

2. THE SYSTEM

2.1 Description

Power to Clarkson SCC from the Bulk Electricity System (BES) is supplied by two separate 28kV/4.16kV transformers via the feeders M4 from Lorne Park TS and M13 from Oakville TS. The location of these feeders in the BES is shown in Figure 1. A simplified one-line diagram of the supply at Clarkson is shown in Figure 2.

For the purposes of the current study, the power supply at Clarkson can be divided into the following groups:

- Class IV supplying all non-critical loads (including office loads).
- Class III feeding essential loads including the primary feeds to the air-conditioning system, control room lighting etc.
- Class II which consists of five uninterruptible power supply (UPS) systems and feeds all critical loads, including the Data Acquisition and Computer System (DACS). This group can be further divided into four subgroups:
  - computer room loads supplied primarily by UPS A and UPS B
  - control room loads supplied by UPS A and UPS B
  - the DACS support systems supplied primarily by UPS C
  - loads supplied by UPS D and UPS E, e.g., power to the circuit breakers.

The 4.16kV supply is stepped down to 600V at two Class IV substations and at two Class III substations. Two cross-ties, one at the 4.16kV level and the other at 600V, are available at the Class IV level. At the Class III level, two diesel generators are available as backups and can assume load in one minute.

Class III power also supplies the UPS systems providing the Class II supply. UPS A, UPS B and UPS C operate at 600V whereas UPS D and UPS E operate at 120/208V supplied by two 600/120/208V transformers fed by two separate Class III feeds. Figure 3 illustrates the details of the UPS A system. Under normal conditions, the AC power is converted to 400V DC by the rectifier and the filtered AC output of the inverter supplies the load. A 400V battery system with a 30-minute capacity is available as back-up if the primary AC power is lost or if the rectifier fails. Note that under most contingencies, the battery system will be required only for a minute or so, ie, until the diesel generators at the Class III level assume load. If the inverter fails, the high speed static switch triggers and the supply is automatically switched over to an alternative source (to UPS C or to a class III source).

This study evaluates the reliability levels of power supply to the above loads as well as at some intermediate points. These points are identified in Figure 2 by the labels *T1*, *T2* ... *T11* and are defined in Subsection 2.2. The definitions are followed by failure criteria for the load points in Subsection 2.3.

2.2 Load Points

As mentioned earlier, two Class IV substations provide power to most non-essential loads at Clarkson. A feed from one of the substations is labeled as load point *T1*. Two cross-ties are available at the Class IV level to ensure continuity of supply. The 4.16kV tie is expected to close in 5 seconds and the 600V tie in 10 seconds. Two Class III substations supply some essential loads such as air conditioning. Load point *T2* is a load supplied by one of the Class III substations and load point *T3* is a load supplied by both the substations. Two standby diesel generators, which start up when both the main feeds fail, serve as backups at this level and are expected to assume load in about 1 minute. Each diesel generator is capable of handling the entire Class III load at Clarkson, in case the other becomes unavailable. A cross tie is available for use when either diesel generator fails.

The output of a UPS and a manual bypass from Class III feed into a metalclad switchgear and three such metalclad switchgears (UPS A, UPS B and UPS C) feed the DACS system. The output of the UPS A switchgear is designated as load point *T4*. The outputs from the UPS A and UPS B switchgears together (two feeds each) supply the computer room via two separate computer distribution frames. The control room is supplied by two feeds, one each from UPS A and UPS B via the two distribution frames mentioned above. UPS C metalclad switchgear supplies the DACS support system (three feeds) via another computer distribution frame. UPS C also serves as a further level of backup for UPS A and UPS B at the input to the computer distribution frame (after a manual switching). The input to a two computer distribution frame feeding the computer and control rooms is termed load point *T5*.

Load point *T6* is defined as any one of the 4 feeds supplying the computer room and load point *T7* refers to two of the four feeds, one each from the two distribution frames. Load point *T8* is defined as any one of the two feeds to the control room and both the feeds together are labeled as load point *T9*. Load point *T10* refers to any one of the 3 feeds supplying the DACS support system. UPS D and UPS E supply most of the critical control power via two computer distribution frames. The output of the UPS D (or UPS E) computer distribution frame is termed load point *T11*.

2.3 Failure Criteria for the Load Points

T1 Loss of power to a load supplied by a feed from a Class IV substation.
T2 Loss of power to a load supplied by a feed from a Class III substation.
T3 Loss of power to a load supplied by feeds from both Class III substations.
T4 Loss of power at the output of the UPS A switchgear.
T5 Loss of power at the input to a computer distribution frame feeding the computer and control rooms.
T6 Loss of any one of the four feeds to the computer room.
T7 Loss of two of the four feeds to the computer room, the two feeds in question being fed via two separate computer distribution frames.
T8 Loss of any one of the two feeds to the control room.
T9 Loss of both the feeds to the control room.
T10 Loss of any one of the three feeds to the DACS support system.
T11 Loss of power at the output of UPS D (or UPS E) computer distribution frame.

3. RELIABILITY EVALUATION

In this study, the mean times between failures, the mean times to restore service, and the probabilities of interruption of power supply to the load points listed in Section 2 are used as indices of reliability of power supply to the System Control Center. The main step in the reliability evaluation is a failure mode and effect analysis /1/.

3.1 Assumptions

- The individual events causing the outages are independent, although some of the events may cause the removal of more than one component from service.
- Overloads and voltage criteria are not considered.
- After a forced outage, the component is isolated by switching.
- Only single and double contingencies are considered.
- Maintenance events (scheduled outages) occur randomly, except that an event is postponed if it would cause a supply interruption.

3.2 Outages considered

- Independent outages of major components. These include:
  - Transmission circuits,
  - Distribution feeders,
  - Circuit breakers,
  - Line terminals,
  - Bus sections,
  - Transformers,
  - Computer distribution frame bus sections,
  - Computer distribution frame breakers,
  - UPS rectifiers,
  - UPS inverters,
  - UPS batteries
- Common mode outages of transmission circuits on common towers
- Failures of breakers to operate when required
- Generator failures

It should be borne in mind that the study does not include the impact of an event such as a fire in the building which might take out several components at once. Such an event will have a significant impact on the computed indices, but the probability of such an event is difficult to assess. Component outage data used in this study are obtained from References 2,3 and 4 and are listed in Appendix A.

3.3 Results

The results of the reliability analysis are presented in Tables 1 to 11 for load points *T1* to *T11* respectively. In the Tables, the results are divided into outages caused by forced outages alone, and outages involving maintenance, ie, outages caused by a forced outage of a backup during a maintenance outage. It should be noted that if the maintenance of a component causes an immediate outage at any of the load points, then this event is not included in the results for that load point, but is included in all 'downstream' calculations. For example, the maintenance of UPS A switchgear causes an immediate outage at load point *T4* and Table 4 does not reflect the impact of this event. However, this maintenance event does affect load point *T6* and the impact is included in the results for load point *T6* in Table 6. A summary of the results is given below.

Load Point	MTBF (years)	Mean Time to Restore	Probability of Outage
T1	2.13	1.46 hrs	$78.5 * 10^{-6}$
T2	208	8.00 hrs	$4.39 * 10^{-6}$
T3	200,000	4.00 hrs	$2.02 * 10^{-9}$
T4	75.4	7.62 hrs	$11.5 * 10^{-6}$
T5	75.3	10.6 min	$0.267 * 10^{-6}$
T6	18.3	12.8 hrs	$79.8 * 10^{-6}$
T7	500,000	3.76 hrs	$0.854 * 10^{-9}$
T8	23.9	8.65 hrs	$41.3 * 10^{-6}$
T9	1,000,000	3.66 hrs	$0.429 * 10^{-9}$
T10	26.0	17.0 hrs	$74.8 * 10^{-6}$
T11	118	4.64 hrs	$4.49 * 10^{-6}$

Note that reliability criteria do not exist for all the load points considered, and evaluation of these results are based on the judgment of the designers and the users. Personnel from the relocation project team have examined these results and have judged them to be acceptable.

4. CONCLUSIONS

A reliability assessment of the power supply at Clarkson has been carried out. The estimated reliability indices were judged to be acceptable by the project relocation department. These figures will form the input to the next phases of the reliability analysis of the Control Center facilities.

REFERENCES

1. J. Endrenyi, "Reliability Modelling in Electric Power Systems", John Wiley, Chicester, 1978.

2. J.N. Harris and C.C. Fong, "Analysis of Equipment Outage Data", TUD Report 0065U, Ontario Hydro, November 1982.

3. D. McColl, "Component Reliability Data for CANDU Nuclear Stations", Ontario Hydro Design & Construction Branch Report 86296, November 1986.

4. P. Cook, "Loss of Supply to the Planned System Control Center", Ontario Hydro unpublished memo, February 1987.

Approved:

A.H. Chung
Manager
Operations Research Department

Submitted:

N. Ramani
Engineer
Reliability and Statistics Section

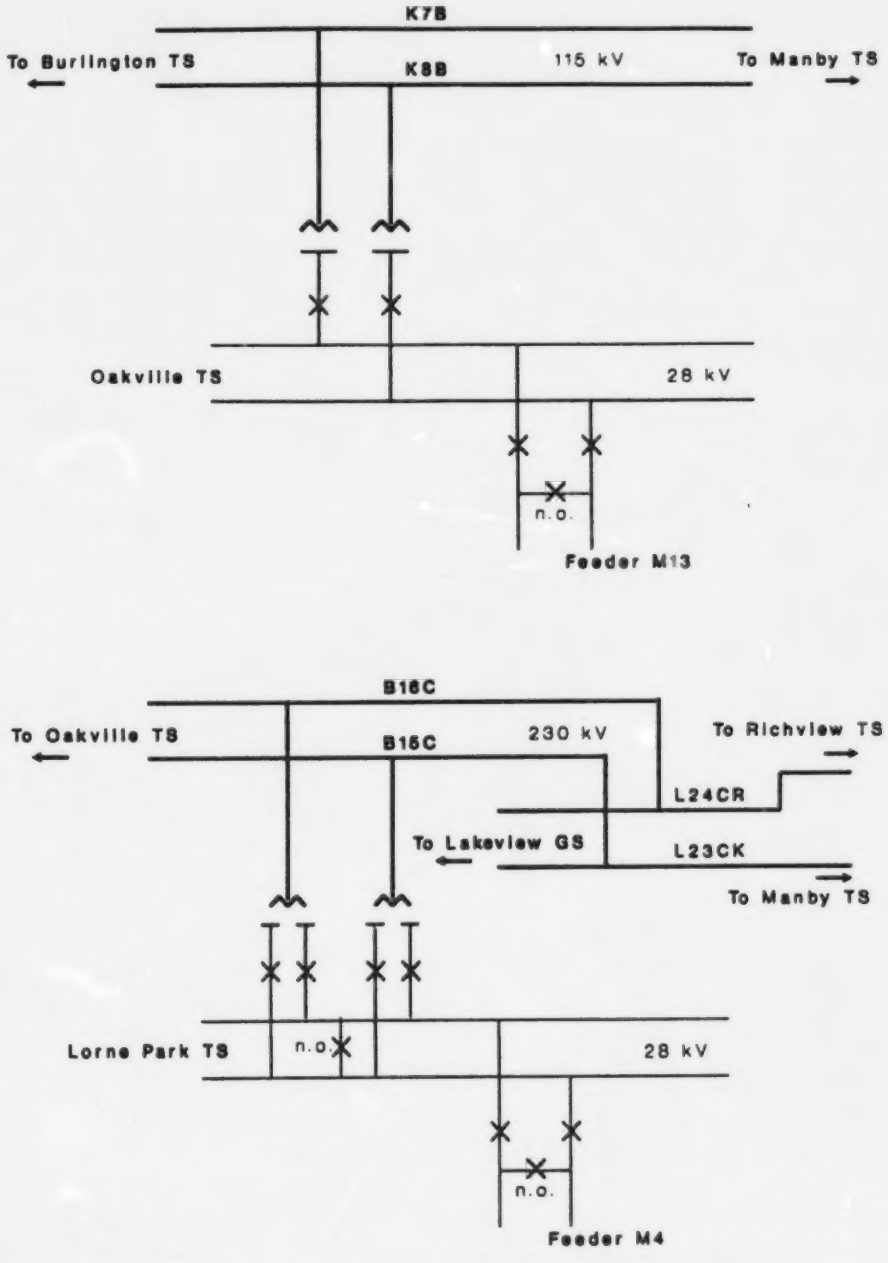


Figure 1 - BES Supply to Clarkson

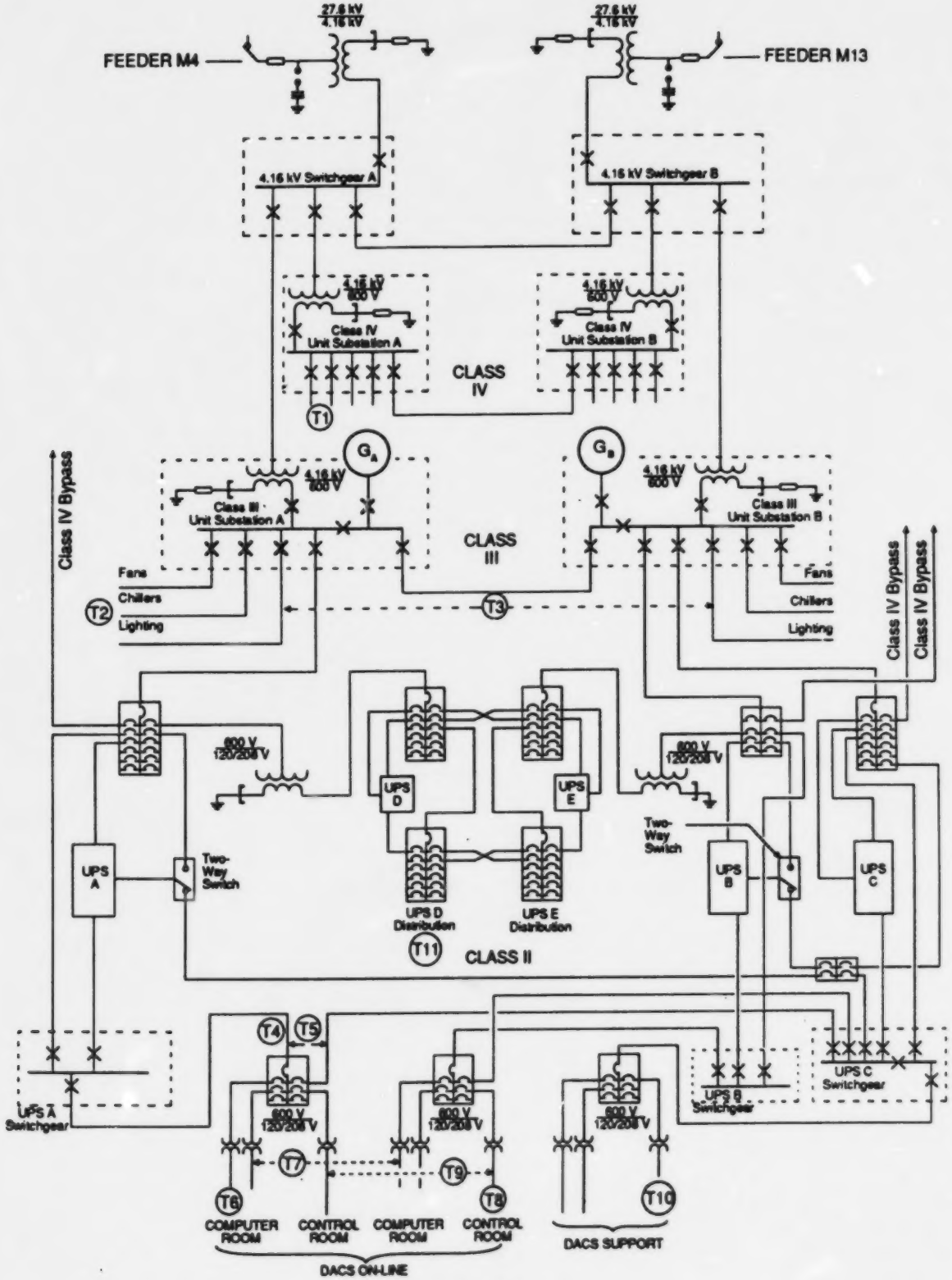


FIGURE 2
CLARKSON SCC

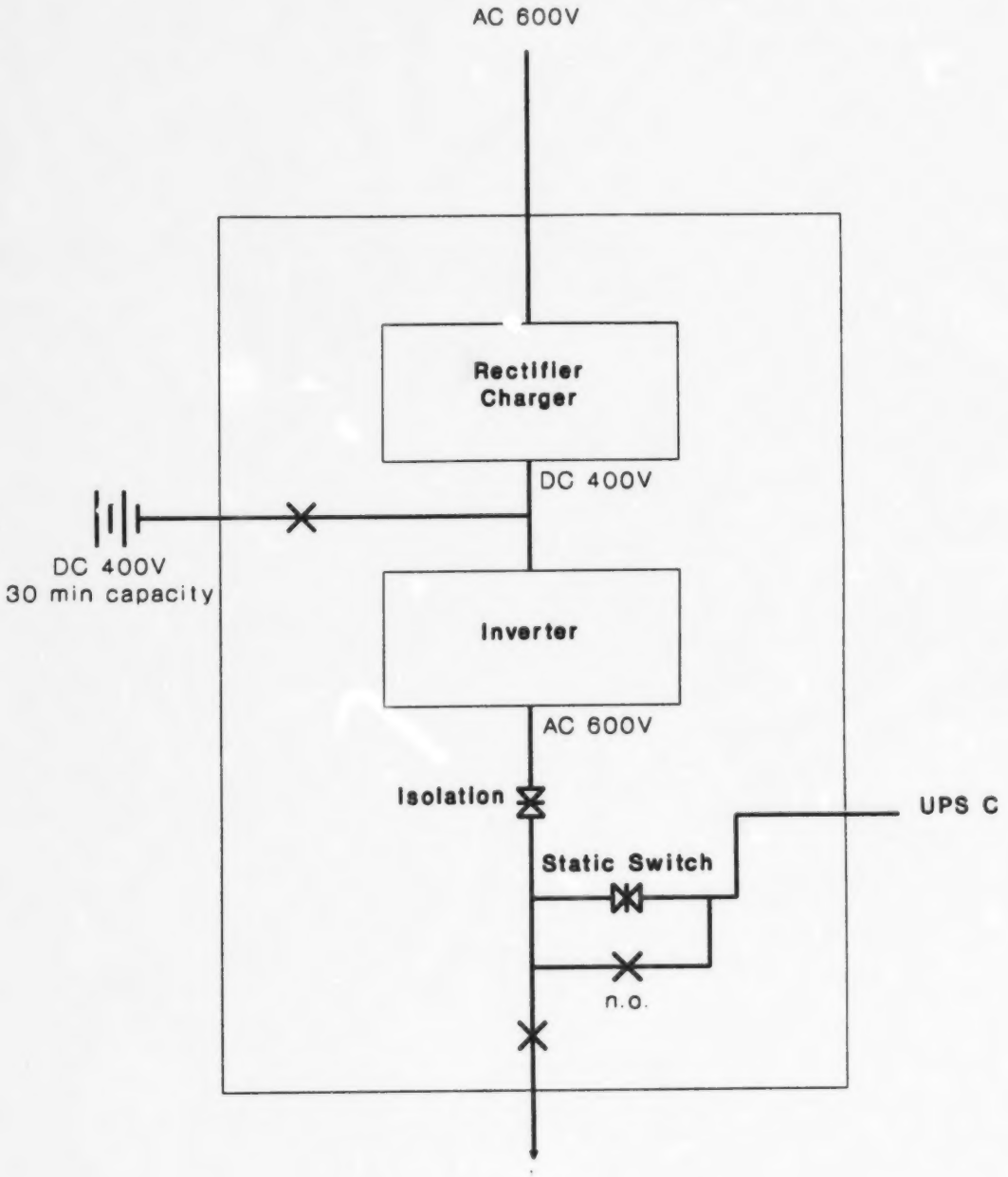


Figure 3 - UPS A

RESULTS

The results of the analysis are presented in the following tables.

Table 1 : Class IV Loads

Table 2 : Class III Loads - Case 1 (one element)

Table 3: Class III Loads - Case 2 (both elements)

Table 4 : UPS A (output of UPS A switchgear)

Table 5 : UPS A (OR) UPS C (Input to a computer distribution frame)

Table 6 : Computer room - Case 1 (Loss of one of the four feeds)

Table 7 : Computer room - Case 2 (Loss of one feed from each distribution frame)

Table 8 : Control room - Case 1 (Loss of one of the two feeds)

Table 9 : Control room - Case 2 (Loss of both feeds)

Table 10 : DACS Support

Table 11 : UPS D and UPS E Loads

TABLE 1

CLASS IV LOADS

Failure Criterion: Loss of power to any given load supplied by one element at the Class IV level.

Reliability Evaluation:

Outage Category	MTBF (years)	Mean Time to Restore	Probability of Outage
Forced Outages - Momentary			
Element A	0.155	1.7 sec	$0.347 * 10^{-6}$
Element B	0.133	2.8 sec	$0.668 * 10^{-6}$
Forced Outages - Sustained	62.7	4.93 hrs	$8.98 * 10^{-6}$
Forced Outage of Backup during Maintenance (see comment 3)	2.20	1.34 hrs	$69.5 * 10^{-6}$
Total - Sustained	2.13	1.46 hrs	$78.5 * 10^{-6}$

Comments:

1. Class IV feeds mostly non-essential loads (office loads etc.). It is assumed that there is no redundancy and the loss of power at a breaker feed at a Class IV substation constitutes a failure.

2. Events contributing significantly to the failure frequency and/or probability include:
   (a) the loss of power at the main feeders (Lorne Park or Oakville)
   (b) the failure of the Class IV substation bus
   (c) the failure of the Class IV substation breaker.

3. Maintenance of the Class IV substations are not included.

TABLE 2

CLASS III LOADS - CASE 1

Failure Criterion: Loss of power to any given load supplied by one element at the Class III level.

Reliability Evaluation:

Outage Category	MTBF (years)	Mean Time to Restore	Probability of Outage
Forced Outages - Momentary			
Element A	0.154	1.8 sec	$0.366 * 10^{-6}$
Element B	0.133	2.9 sec	$0.686 * 10^{-6}$
Forced Outages - Sustained	208	8.00 hrs	$4.38 * 10^{-6}$
Forced Outage of Backup during Maintenance (see comment 4)	300,000	4.00 hrs	$0.002 * 10^{-6}$
Total - Sustained	208	8.00 hrs	$4.39 * 10^{-6}$

Comments:

1. Class III feeds critical loads such as air conditioning.
2. On-site standby generation is available for back up.
3. Events contributing significantly to the failure frequency and/or probability include:
   (a) the loss of power at one or both the feeders (Lorne Park and Oakville)
   (b) the failure of the Class III substation bus
   (c) the failure of the Class III substation breaker.
4. Maintenance of the class III substations are not included.

TABLE 3

CLASS III LOADS - CASE 2

Failure Criterion: Loss of power to any given load supplied by both elements at the Class III level.

Reliability Evaluation:

Outage Category	MTBF (years)	Mean Time to Restore	Probability of Outage
Forced Outages - Momentary	100	1.0 min	$19.0 * 10^{-9}$
Forced Outages - Sustained	$2 * 10^{7}$	3.84 hrs	$0.02* 10^{-9}$
Forced Outage of Backup during Maintenance	200,000	4.00 hrs	$2.00 * 10^{-9}$
Total - Sustrined	200,000	4.00 hrs	$2.02 * 10^{-9}$

Comments:

1. At the Class III level, there is full redundancy in most cases and the two elements feed identical loads. This case analyses the case where both elements and both the diesel generators fail.

TABLE 4

UPS A

Failure Criterion: Loss of power at the output of UPS A metalclad switchgear

Reliability Evaluation:

Outage Category	MTBF (years)	Mean Time to Restore	Probability of Outage
Forced Outages - Sustained	75.5	7.62 hrs	$11.5 * 10^{-6}$
Forced Outage of Backup during Maintenance (see comment 4)	60,000	4.00 hrs	$0.008 * 10^{-6}$
Total - Sustained	75.4	7.62 hrs	$11.5 * 10^{-6}$

Comments:

1. All the UPS systems are backed up by a battery with a capacity of 30 minutes at full load.

2. If the UPS A inverter fails, an automatic bypass switch transfers control to UPS C.

3. Events contributing significantly to the failure frequency and/or probability include:
   (a) the failure of the 600V metalclad switchgear bus
   (b) the failure of the 600V metalclad switchgear breaker.

4. Maintenance of the UPS A metalclad switchgear is not included.

TABLE 5

UPS A (OR) UPS C

Failure Criterion: Loss of power at the input to a computer distribution frame supplying the computer and control rooms

Reliability Evaluation:

Outage Category	MTBF (years)	Mean Time to Restore	Probability of Outage
Forced Outages - Switching	75.5	10.0 min	$0.252 * 10^{-6}$
Forced Outages - Sustained	74000	3.90 hrs	$0.006 * 10^{-6}$
Forced Outage of Backup during Maintenance	48000	3.89 hrs	$0.009 * 10^{-6}$
Total	75.3	10.6 min	$0.267 * 10^{-6}$

Comments:

1. The computer and control rooms are supplied by two computer distribution frames fed by UPS A and UPS B metalclad switchgears respectively. In case of failure of supply from either of the switchgears, a manual transfer is made to UPS C switchgear. This case examines the logical "OR" of the two inputs UPS A and UPS C, ie, the possibility of loss of power to a distribution frame.

TABLE 6

COMPUTER ROOM - CASE 1

Failure Criterion: Any interruption to any of the four feeds to the computer room

Reliability Evaluation:

Outage Category	MTBF (years)	Mean Time to Restore	Probability of Outage
Forced Outages - Switching	37.7	10.0 min	$0.504 * 10^{-6}$
Forced Outages - Sustained	35.7	24.8 hrs	$79.3 * 10^{-6}$
Forced Outage of Backup during Maintenance	24000	3.89 hrs	$0.019 * 10^{-6}$
Total	18.3	12.8 hrs	$79.8 * 10^{-6}$

Comments:

1. There are four lines available for the computer room fed via two separate computer distribution frames. Loss of power to any one of the four feeds is evaluated here.

2. Events contributing significantly to the failure frequency and/or probability include:
   (a) the failure of any of the UPS systems
   (b) the failure of a 600/120/208V transformer
   (c) the failure of the computer distribution frame bus
   (d) the failure of the computer distribution frame breaker.

TABLE 7

COMPUTER ROOM - CASE 2

Failure Criterion: Loss of power to two of the four feeds to the computer room, the two feeds in question being fed via two separate computer distribution frames.

Reliability Evaluation:

Outage Category	MTBF (years)	Mean Time to Restore	Probability of Outage
Forced Outages - Switching	700,000	10.0 min	$0.026 * 10^{-9}$
Forced Outages - Sustained	1,600,000	11.8 hrs	$0.828 * 10^{-9}$
Total	500,000	3.76 hrs	$0.854 * 10^{-9}$

Comments:

1. There are four lines available for the computer room fed via two separate computer distribution frames. Loss of two of the feeds is particularly critical, ie, recovery is not possible via a simple reconfiguration, when the two feeds are being fed via two separate distribution frames. This event is analyzed here.

2. There is considerable redundancy available in the system and thus most failure events are cleared by switching. Thus, the probability of the above event is very small.

TABLE 8

CONTROL ROOM - CASE 1

Failure Criterion: Any interruption to any of the two feeds to the control room

Reliability Evaluation:

Outage Category	MTBF (years)	Mean Time to Restore	Probability of Outage
Forced Outages - Switching	37.7	10.0 min	$0.504 * 10^{-6}$
Forced Outages - Sustained	65.7	23.4 hrs	$40.7 * 10^{-6}$
Forced Outage of Backup during Maintenance	24000	3.89 hrs	$0.019 * 10^{-6}$
Total	23.9	8.65 hrs	$41.3 * 10^{-6}$

Comments:

1. There are two lines available for the control room fed via two separate computer distribution frames. Loss of power to any one of the two feeds is evaluated here.

2. Events contributing significantly to the failure frequency and/or probability include:
   (a) the failure of any of the UPS systems
   (b) the failure of a 600/120/208V transformer
   (c) the failure of the computer distribution frame bus
   (d) the failure of the computer distribution frame breaker.

TABLE 9

CONTROL ROOM - CASE 2

Failure Criterion: Loss of power to both the feeds to the control room

Reliability Evaluation:

Outage Category	MTBF (years)	Mean Time to Restore	Probability of Outage
Forced Outages - Switching	1,400,000	10.0 min	$0.014 * 10^{-9}$
Forced Outages - Sustained	3,200,000	11.7 hrs	$0.415 * 10^{-9}$
Total	1,000,000	3.66 hrs	$0.429 * 10^{-9}$

Comments:

1. There are two lines available for the control room fed via two separate computer distribution frames. Loss of both the feeds is evaluated here.

2. There is considerable redundancy available in the system and thus most failure events are cleared by switching. Thus, the probability of the above event is very small.

TABLE 10

DACS SUPPORT

Failure Criterion: Loss of power to any one of the three feeds to the DACS Support system (fed primarily by UPS C)

Reliability Evaluation:

Outage Category	MTBF (years)	Mean Time to Restore	Probability of Outage
Forced Outages - Sustained	26.0	17.0 hrs	$74.8 * 10^{-6}$
Forced Outage of Backup during Maintenance (see comment 3)	24,000	4.00 hrs	$0.02 * 10^{-6}$
Total	26.0	17.0 hrs	$74.8 * 10^{-6}$

Comments:

1. The support services are fed by three lines and it is assumed that the loss of any one of these lines constitutes a failure.

2. Events contributing significantly to the failure frequency and/or probability include:
   (a) the failure of the UPS C system
   (b) the failure of the 600/120/208V transformer
   (c) the failure of the computer distribution frame bus
   (d) the failure of the computer distribution frame breaker.

3. Maintenance of the UPS C switchgear is not included.

TABLE 11

UPS D AND UPS E LOADS

Failure Criterion: Loss of power for the loads fed by UPS D and UPS E

Reliability Evaluation:

Outage Category	MTBF (years)	Mean Time to Restore	Probability of Outage
Forced Outages - Switching	278	10 min	$0.07 * 10^{-6}$
Forced Outages - Sustained	208	8.00 hrs	$4.38 * 10^{-6}$
Forced Outage of Backup during Maintenance	15,000	4.62 hrs	$0.04 * 10^{-6}$
Total	118	4.64 hrs	$4.49 * 10^{-6}$

Comments:

1. UPS D and E feed several critical loads such as control power for all the breakers, emergency lighting and essential telemetry.

2. The UPS systems are backed up by a battery with a capacity of 30 minutes.

3. It is assumed that loss of power at the computer distribution frame is a failure and any redundancies at the load level are not accounted for.

4. Events contributing significantly to the failure frequency and/or probability include:
   (a) the failure of the 600V computer distribution frame bus
   (b) the failure of the 600V computer distribution frame breaker
   (c) the failure of the 600/120/208V transformer
   (d) the failure of the computer distribution frame bus
   (e) the failure of the computer distribution frame breaker.

APPENDIX A

OUTAGE DATA

This Appendix lists the outage data used in this study. Most of the data were obtained from References 2, 3 and 4.

Transmission Lines
(per 100 km)

Component or Mode	Outage Frequency (/yr)		Outage Duration (hrs)
	Normal Weather	Adverse Weather	
230kV			
Permanent	0.04	4.23	11.2
Temporary	0.04	24.67	0.1067
Transient	0.05	51.08	0.0042
115kV			
Permanent	0.15	17.31	12.6
Temporary	0.22	112.49	0.075
Transient	0.48	38.32	0.0042
Common mode 230kV			
Permanent	0.009	2.15	11.2
Temporary	0.0	10.75	0.1067
Transient	0.0	9.89	0.0042
Common mode 115kV			
Permanent	0.0	0.69	12.6
Temporary	0.014	22.08	0.075
Transient	0.0	68.99	0.0042
28kV Feeder	0.1436	0.1436	1.258
M4 Transient*	5	5	0.0003
M13 Transient*	3	3	0.0003

* Note: These figures are not system averages, but are based on component specific data provided to the SCC Relocation Department by the Regions Branch. Also, the numbers refer to the whole feeders, and are not per 100km.

Transformers

Component or Mode	Outage Frequency (/yr)		Outage Duration (hrs)
	Normal Weather	Adverse Weather	
230kV/28kV	0.114	0.114	142
115kV/28kV	0.114	0.114	142
28kV/4.16kV	0.013	0.013	50
4.16kV/600V	0.0053	0.0053	50
600V/120V	0.0028	0.0028	50

Bus Sections

Component or Mode	Outage Frequency (/yr)		Outage Duration (hrs)
	Normal Weather	Adverse Weather	
230kV or 115kV			
Permanent	0.012	2.817	13.3
Temporary	0.008	0.352	0.355
28kV	0.0649	0.0649	8
4.16kV	0.0167	0.0167	15
600V	0.0012	0.0012	8
120V	0.0012	0.0012	8

Circuit Breakers

Component or Mode	Outage Frequency (/yr)	Outage Duration (hrs)
230kV	0.0074	249.6
115kV	0.0025	249.6
4.16kV	0.0082	10
600V	0.0036	8
120V	0.0036	8

UPS components
(600V and 120V)

Component or Mode	Outage Frequency (/yr)	Outage Duration (hrs)
Rectifier	0.044	12
Inverter	1.25	8
Battery	0.0014	8
Static Switch	0.0036	8
Breaker	0.0036	8

Maintenance Data

Component or Mode	Outage Frequency (/yr)	Outage Duration (hrs)
Transmission Line	0.0056/km	114
Line Terminal	0.3274	72.9
Circuit Breaker	0.1933	82.0
Bus Section	0.2862	73.6
Tap Transformer	0.4507	98.3
Class IV / III Substation	1.0	8.0
Metalclad Switchgear	1.0	8.0
UPS	1.0	8.0

Miscellaneous

Probability of a breaker failing to open = 0.0005

Probability of a normally open breaker failing to close = 0.0005

Time for an open breaker to close
- auto (Class IV tie) = 5 sec
- auto (Class III tie) = 10 sec

Time for an open breaker to close
- manual = 10 min

Probability of generator start failure = 0.02

Time for the generator to be on-line = 1 min